EXPORTING TECHNOLOGY AND SOFTWARE, PARTICULARLY ENCRYPTION

Benjamin H. Flowe, Jr.

October 11, 2013

Exporting Technology and Software, Particularly Encryption

Benjamin H. Flowe, Jr.[1]

This article is an overview of export controls on dual-use technology under the Export Administration Regulations, 15 C.F.R. §§ 730 *et seq.* ("EAR"), and the sanctions regulations administered by the Treasury Department's Office of Foreign Assets Controls ("OFAC"), 31 C.F.R. § 500 *et seq.* This version addresses some aspects of technology controls under the International Traffic in Arms Regulations, 22 C.F.R. §§ 120 *et seq.* ("ITAR"), but not in depth. The article first provides basic guidance on controls over technology and software, second summarizes the so-called "deemed export" rule and related issues, third analyzes current export controls on encryption software, hardware, and technology , and fourth offers insights into applying export controls in e-commerce and "cloud" computing environments.

1. BASIC GUIDANCE FOR CONTROLLING EXPORTS OF TECHNOLOGY AND SOFTWARE

The law and government policies concerning technology and software are complex. This discussion summarizes the current rules and special procedures for handling exports of technology and software. A company's export compliance administrators should be consulted before exporting any technology or software that is not in the public domain or listed on a company's Export Control Product Matrix.[2]

1.1. TECHNOLOGY.[3] **In general, five basic categories of technology determine applicable export controls. This assumes that one is exporting "technology" as defined in the EAR (e.g., does not include general business correspondence that does not meet this definition). All technology directly related to items listed on the ITAR's U.S. Munitions List require export authorization for all destinations from the State Department's Directorate of Defense Trade Controls ("DDTC") . Other provisions in this analysis will not apply to ITAR technology.** This analysis also assumes that an exporter screens to avoid General Prohibitions 4 through 10 on unlawful exports for certain end-uses and to certain end-users, including denied parties. EAR § 736.2(b)(4) -(10).

1.1.1. 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 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 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).

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 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 article. 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 Internet, or donate manuals and other materials to a library to satisfy the publication requirement. However, 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 subjecting such technology to confidentiality agreements or other restrictions in other contexts, which could undercut the notion that it is truly "published." The facts in the application of the public availability exemption are often the most nettlesome issue.

ITAR § 120.10(a)(5) similarly excludes from the term "technical data" information concerning general scientific, mathematical or engineering principles commonly taught in schools, colleges and universities and information in the public domain as defined in § 120.11. It also does not include basic marketing information on function or purpose or general system descriptions of defense articles. Practitioners sometimes debate whether information found on the Internet qualifies as "public domain" under the ITAR because the regulations still do not mention the Internet as a mode of publication, but the primary ITAR definitions do generally overlap with EAR definitions . The better view on this debate, in this author's opinion, is that information freely available on the Internet is in the public domain.

The OFAC Sanctions Regulations similarly exempt "informational materials" from regulation, based on the so-called Berman Amendments to the Trading with the Enemy Act and the International Emergency Economic Powers Act. The OFAC Sanctions Regulations exclude from the scope of exempt "informational materials" any information that is controlled as EAR or ITAR "technology," implying that information that is exempt under EAR or ITAR public domain concepts may qualify as exempt "informational materials." Thus, qualifying public domain technology (and, we believe, software) is exempt from export controls even to Embargoed Countries (currently Cuba, Iran, North Korea, North Sudan, and Syria).

1.1.2. 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 License Exception TSU to any country (except Iran and likely Sudan), 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), 746.7.

1.1.3. 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 Iran and likely Sudan). EAR §§ 740.13(a), 746.7. 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, Supp. No. 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.

1.1.4. Fourth, to the extent that TSPA or TSU are not available, all technology to be exported must be **classified under the applicable Export Control Classification Number ("ECCN")** in the Commerce Control List ("CCL") set forth in Supp. No. 1 to EAR Part 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, TSU, CIV, or CTP may be used for the export to a particular destination.

A. If no ECCN is applicable (EAR99) or the application of the data's ECCN to the Country Matrix in Supp. No. 1 to EAR Part 738 shows No License is Required, the data may be exported under NLR to all appropriate destinations except the Embargoed Countries;

B. If the applicable ECCN states "TSR: Yes" then it may be exported under License Exception TSR only to destinations in Country Group B (Supp. No. 1 to EAR Part 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).

C. If the applicable ECCN has a license requirement to the ultimate destination for National Security ("NS") reasons only and states "CIV – Yes," then the applicable technology may be exported to civil end-users for civil end-uses in Country Group D:1, except North Korea. EAR § 740.5. The performance metric for such microprocessor technology controlled by ECCN 3E002 in 2007 retired the old "MTOPS" standard, substituting composite theoretical performance ("CTP") metrics keyed to the new "Weighted TeraFLOPS" (WT) standard in effect for computers controlled under ECCNs 4A003 and 4A994 on the CCL, implementing Wassenaar Arrangement changes. 72 *Fed. Reg.* 62524 (Nov. 5, 2007).

D. If the applicable technology or software is controlled by ECCNs 4D001 or 4E001 and is specially designed or modified for the "development", "production", or "use" of computers, including "electronic assemblies" and specially designed components therefor classified in ECCN 4A003, except ECCN 4A003.e (equipment performing analog-to-digital conversions exceeding the limits in ECCN 3A001.a.5.a) or is controlled for missile technology (MT) reasons, then it may be exported under License Exception APP to Computer Tier countries as provided in EAR § 740.7. This License Exception (formerly known as CTP) was previously restricted to deemed exports with similar Foreign National Review requirements, and was in 2005 broadened to allow exports of the same technology to applicable countries due to the

agreement by Wassenaar Arrangement members in December 2004 to decontrol similar levels of technology. (70 *Fed. Reg.* 41094 (Jul. 15, 2005).)

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 "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 as they collaborate with colleagues around the world and foreign nationals.

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.[4]

When considering whether technology constitutes controlled "use" technology, it is important to consider the 2006 interpretation of the term issued by BIS, in the context of its review of the scope of deemed export controls (discussed in detail in the next section.) "Use" technology is defined to include: "Operation, installation (including on-site installation), maintenance (checking), repair, overhaul and refurbishing." (EAR § 772, definition of "use".)

Commerce has issued an interpretation that technology does not meet the definition of "use" technology" unless it encompasses all six of the aforementioned types of information. (71 *Fed. Reg*. 30840, at 30842 (May 31, 2006). Thus, unless the proposed export involves a comprehensive set of use-related technical data, including overhaul and refurbishment technology, the likelihood of a license requirement is greatly diminished.

Some recent ECCNs that control some or all of these six aspects of technology, however, do not use the defined term "use." ECCN 7E003, for example, controls technology for the "repair, refurbishing, or overhaul" of certain equipment, but omits operation, installation, and maintenance. Technology ECCNs in the so-called "600 Series," which are entering the CCL in connection with the transfer of items from the ITAR to the EAR, control technology for the "operation, installation, maintenance, repair, refurbishing, **or** overhaul" of controlled items, rendering the 2006 "use" interpretation inapplicable to such ECCNs. This revised wording is apparently deliberate, as control over any of these six elements is consistent with the approach to ITAR technical data controls, and both DDTC and BIS have repeatedly stated in the context of the ongoing export control reform process that they intend to shift controls of defense articles to the EAR, and not to decontrol such items. In Wassenaar negotiations over ECCN revisions, officials decided against revising the definition of "use" to roll back what many viewed as a unilateral change, but are addressing in each revised ECCN whether and to what extent to control any of the elements of "use," usually omitting any on operation or maintenance.

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, Note 1.)

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.
> EAR § 774, Supp. No. 2, Note 1.

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 3 WT (or other applicable control parameters).

One expert applying the term "required" might say that, because all technology to develop or produce controlled computers also is used to develop or produce 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 some technology that is 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. Deeper level analysis is required to determine just what are the specific technologies that are "peculiarly responsible" for producing end products that achieve technical specifications that exceed the ECCN 4A003 control parameters.

Then, 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. Likewise, all "required" technologies might be publicly available and thus not controlled. 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 WT for TSR exports controlled by ECCN 4E001.

1.1.5. 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 Supp. No. 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 EAR. (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 within a class of "protected persons," such as asylees and refugees; or in the case of reexports, is not a citizen or permanent resident under the laws of the location of "deemed reexport."

1.2. SOFTWARE. Export administrators should use the following line of analysis to determine the proper licensing requirements for particular software products to specific destinations. Points 1.2.5 through 1.2.9 apply to most software programs, and most non-crytpographic software currently qualifies for export under NLR or License Exception TSU to all destinations except Embargoed Countries.

1.2.1. 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 ITAR software.** Commercial software that contains certain encryption functions (with a few exceptions for authentication, access control, and decryption-only proprietary software protection routines) was covered by the ITAR until December 30, 1996. Now, such items are subject to the EAR, with the level of restriction depending on the type of item and functionality. More sensitive encryption items are often subject to stringent licensing or prior U.S. government review requirements.

1.2.2. Software that is **publicly available** at no charge other than cost of reproduction and distribution, such as in a library or on a public web site, may be exported to any destination without a License (using TSPA, as described above for technical data). **Note that certain encryption software is not eligible for this exclusion. See Section 3.3.5 below for a discussion of controls applicable to U.S.-origin publicly available encryption software.**

1.2.3. All software programs not eligible for TSPA exports that are exported to **Embargoed Countries** require a License either from BIS or under the OFAC sanctions regulations for those destinations.

1.2.4. 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 and firearms, but may be expanded to include items related to missiles.

1.2.5. Most software subject to the EAR is **classified under an ECCN** on the CCL. 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 the **Embargoed Countries**. (See 1.2.9 below and classification discussion above.) Note that exports to Iraq and Libya are not embargoed anymore but are subject to stricter controls than most countries.

1.2.6. Mass-Market Software. Software, regardless of classification under the CCL, may be exported to all destinations except for the Embargoed Countries under License Exception TSU if it isgenerally available to the public by being:

A. Sold from stock at retail selling points (without being sold only bundled with hardware) by means of:

(1) Over the counter transactions;
(2) Mail order transactions;
(3) Electronic transactions; or
(4) Telephone call transactions; and

B. Designed for installation by the user without further substantial support by the supplier (telephone/IM chat, etc. help lines are not a problem).

EAR § 740.13(d) and the General Software Note in Supp. No. 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 cryptographic functions should be exported as mass-market software without complying with the encryption export control regime discussed below.**

1.2.7. 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 (except for Iran and Sudan). (EAR §§ 740.13(a)/746.7.) 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.

1.2.8. 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 (with the possible exception of Iran and Sudan), provided that such updates are provided to the same consignee and do not enhance the specified functional capabilities of the initially licensed software package. (EAR § 740.13(c).)

1.2.9. 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 for export to all but Embargoed Countries under the designator NLR. **If none of the above described License Exception Provisions 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 it must be exported under a License to a particular destination.

A. Classify the software. Software is specifically covered under 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, usually because it is related to the "production," "development," or "use" of CCL controlled items.

B. If EAR99 applies or the applicable ECCN "Requirements" section combined with the Country Matrix in EAR Part 738, Supp. No. 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 Embargoed Countries, any others specified in the applicable ECCN or the Country Matrix. This assumes that other screens (e.g., denial lists and proliferation end-user/s) are cleared.

C. If an applicable ECCN states "TSR: Yes", then it may be exported under License Exception TSR to destinations in Country Group B (Supp. No. 1 to EAR Part 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.

D. License Exceptions TSU and ENC 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, and APR).

E. See Part 1.1.4.D above for rules applicable to exports of software controlled by ECCN 4D001 specially designed or modified for the "development", "production", or "use" of computers, including "electronic assemblies" and specially designed components therefor classified under ECCN 4A003.

F. 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.

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

1.3. 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 guidance to minimize TSR reporting, given that technical data exports are often repetitive. First, one does **not** need to report "deemed exports" to foreign nationals in the U.S. Second, exporters need only report the 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 the same end-user only if scope of controlled technology changes. **No reports of reexports under other License Exceptions or NLR are required by Part 743.**

1.4. 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 Export 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.)

Some clients have created matrices of the types of technologies that would require a license for export to (a) Country Group B destinations even if a License Exception TSR written assurance is in place, or (b) a subset of those countries for which License Exception TSR is more broadly applicable. These can be helpful to alert research and development personnel when they might cross the line. It is difficult to classify technology and software and sometimes easier for

such groups to have a clearer idea of what might require a license when working with their main affiliate offices.

2. FURTHER EXPLORATION OF THE "DEEMED EXPORT" RULE

The U.S. high-tech industry, faced with shortages of technically trained employees, hires thousands of foreign nationals annually. Many come 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). In some cases, the employer must obtain export licenses 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 the PRC or Country Group E)), but it applies to all foreign nationals who have access to technology or source code that would require a license for 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 BIS enforcement of deemed export violations , perhaps due to pressure stemming from critical reports of the Commerce Department Inspector General and high-level BIS attention to the issue that followed.

2.1. 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 already existed in 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.) Nonetheless, deemed export violations carry the same penalties as any other EAR 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.

Companies must determine to what technical data foreign nationals will have access, then to classify that data under the correct ECCN on the CCL. The 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), License Exception TSU, or another available License Exception. 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 a deemed export license is required depends on a foreign national's country of citizenship and which of the Country Groups in Supp. 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 the PRC, Russia, several former republics of the USSR, 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 form of written assurance that they will not re-export 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 form of 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 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 in the United States.) 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, due to the availability of License Exceptions. 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 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. The Clinton and Bush Administrations resisted making this change, although BIS published a Proposed Rule to establish License Exception ICT in the fall of 2008. 73 *Fed. Reg.* 57554 (Oct. 3, 2008). The overwhelming comments from potential users were that the restrictions in the proposed version of the rule made the proposed mechanism more restrictive than obtaining individual licenses; so, it awaits further review.

When, at the end of 1996, Commerce made it clear that it would start enforcing the deemed export rule, many more firms rushed to obtain export licenses for the foreign nationals they sought to hire. The Department of Defense, a key player in the interagency group that is responsible for licensing, grew alarmed by the flood of export license applications in the first few months of 1997 (clearly, only the tip of the iceberg) and began applying closer scrutiny to these applications. A backlog of applications quickly amassed. Commerce, recognizing the problems

with the deemed export rule and the backlog of applications, requested the cabinet-level Export Administration Review Board ("EARB") to meet in June 1997, for the first time in seven years. The EARB is the last level of interagency export control dispute resolution before the President. It is composed of the Secretaries of the Departments of State, Commerce, Defense, Energy, Justice (for encryption products), and (at that time) the Director of the Arms Control and Disarmament Agency. The non-voting Chairman of the Joint Chiefs of Staff and the Director of the CIA advise the EARB. The Commerce Department was proposing to change the "deemed export" control rule back to the "knowledge" or "intent" based rule of pre-1994.

When the EARB meeting was postponed for unrelated reasons, a sub-cabinet working group released, in 1997, 14 guidelines called Standard License Conditions for Foreign Nationals, which were revised at the beginning of 1999. These guidelines were primarily designed for the semiconductor and computer industries, which accounted for the vast majority of "deemed export" license applications. Additional standard conditions were released for encryption items. (These standard conditions have periodically been revised, and are available as part of the application guidelines on the BIS web site at http://www.bis.doc.gov/deemedexports/foreignationals.pdf.)

In 1997, the standard conditions enabled Commerce to process the backlog of cases that had developed and to diminish the political pressure to change the rule. Clearly, the Administration hoped that approving most licenses with standard conditions would rid them of industry's furor over the "deemed export rule". This was in vain. U.S. industry has complained that, although about 99 percent of deemed export applications are eventually approved by BIS, the licenses contain numerous conditions which, in reality, require employers to change the job descriptions of the foreign nationals they seek to hire.

More fundamentally, 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.)

It has been difficult to change the rule because of potential political repercussions, particularly in the wake of 1999's Cox Committee Report -- which focused in part on alleged deemed export violations by Energy Department laboratories -- as well as Inspectors General Reports in 1999 and again in March 2000 alleging that enforcement is inadequate. Some have been concerned about the high number of PRC graduates from engineering schools that were joining U.S. companies. Many exporters worked with the Bush Administration and Congress to achieve reductions to the deemed export rule and other technology transfers, either to eliminate it or, more likely, to obtain broader License Exception treatment for transfers of most data to affiliates, as was done for encryption technology. The Regulations and Procedures Technical

Advisory Committee ("RPTAC") to BIS (of which this author has long been a member) is one of many groups continuing to propose a License Exception for intracompany transfers of technologies in a manner similar to License Exception ENC for encryption technologies and source code.

After the September 11, 2001, terrorist attacks against the United States, wholesale reform proposals stalled, but the proposal for intra-company transfers continued. That effort stalled in 2004 because the proposal as revised by agencies became burdened with so many restrictions that most electronics companies advised they would not find it useful. BIS also proposed in 2003 raising thresholds of technology requiring licenses related to development and production of computers and microprocessors (68 *Fed. Reg.* 60891 (Oct. 24, 2004), and implemented this proposal in November 2004, but in a more limited way so far applicable only to deemed exports after a Foreign National Review submission has been made for the foreign nationals as described in Parts 1.1.4.C and D above.

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 certain 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. http://www.oig.doc.gov/OIGPublications/IPE-16176.pdf

In response to a 2004 report by the Commerce Department Office of the Inspector General ("OIG") critical of the EAR's current deemed export rule, BIS issued a request for comments regarding the potential impact of the OIG's proposed changes to the deemed export rule. 70 *Fed. Reg.* 15607 (Mar. 28, 2005). The chief concern to exporters in the OIG's suggested changes was the recommendation that BIS adopt a policy of determining the nationality of a foreign national based on their country of birth, a departure from the current BIS practice of using the most recent country where the foreign national has gained citizenship of the equivalent of permanent residency. The OIG proposed the change as a means of imposing a license requirement on persons born in sensitive countries, like China, Russia, and India, who have obtained permanent residency in Canada, the European Union, or another country where a license are not required for sensitive dual-use technology, out of fear that such persons will exploit the lack of a deemed export license requirement to obtain sensitive technology and export it to their country of birth. Secondary issues recommended by the OIG relate to clarifications to the definition of "use" technology to eliminate a grammatical error that could lead to confusion, and clarifications to some of the guidance provided in the EAR about whether activities constitute "fundamental research" that is not subject to the EAR.

Industry and academia responded with the most comments ever on a proposed or interim EAR amendment (over 300) on the BIS Federal Register notice of March 28, 2005 (with a clarification notice following on June 27, 2005). Virtually all of the comments opposed the proposed changes in one way or another. The academic community took aim primarily at proposed changes to the "fundamental research" definition in the EAR and the proposal that deemed export licenses be required for foreign nationals with mere access to export controlled equipment. Industry took primary aim at the change proposed by the Commerce Department's

Inspector General that a foreign national's country of birth be used as the nationality criterion for license determinations. We assisted several clients in preparing comments and also contributed to comments submitted by the American Bar Association. All comments are available at http://efoia.bis.doc.gov/index.php/component/docman/doc_view/724-advance-notice-of-proposed-rulemaking?Itemid=526.

Following a Financial Times article quoting then-Under Secretary for Industry and Security David McCormick as seeking to take "a more prudent approach" to making changes to the administration of the "deemed export" rule, BIS formally withdrew an advance notice of proposed rulemaking concerning proposed changes. 71 *Fed. Reg.* 30840 (May 31, 2006). Many were surprised that BIS refrained from making a few of the less controversial modifications to the deemed export regulations, instead choosing a more collaborative approach by forming a new advisory committee (with a one year life span) to assist BIS in formulating revised deemed export policies on. *See* 71 *Fed. Reg.* 29301 (May 22, 2006). The Deemed Export Advisory Committee ("DEAC") was formed in September of 2006, and included a number of high-level members of industry, academia, and former government officials. The DEAC held a number of consultative sessions around the country during 2006 and 2007, inviting representatives of industry and academia to make presentations and submit their recommendations for deemed export reform. The DEAC issued its report in December of 2007, making several recommendations for reforming the deemed export rule.

The recommendations were high-level, suggesting that BIS expand its educational outreach due to lack of awareness of the deemed export rule; modify the scope of technology that is subject to the deemed export rule to focus on more critical technologies; set up a "Trusted Entities" program to allow U.S. industry and academic institutions to get entity-wide licenses; base licensing not on the most recently acquired citizenship or permanent residency of a foreign national, but on a more balanced test of an individual's loyalty; establish an advisory committee to review and "sunset" controls on technology; and re-define a number of the terms used to define the scope of "fundamental research" to clarify the scope of controls.

BIS responded to the DEAC report by establishing an Emerging Technologies Advisory Committee, with the aim of identifying emerging technologies for potential regulation, as well as by expanding its educational and outreach programs on technology controls. BIS also issued a notice requesting comments on two of the DEAC's specific recommendations: (1) the narrowing the scope of the application of the deemed export rule to only some of the technology listed on the Commerce Control List and (2) the use of a more comprehensive "loyalty" test in assessing license requirements for foreign nationals. 73 *Fed. Reg.* 28795 (May 19, 2008). Comments on these proposals can be accessed at http://efoia.bis.doc.gov/pubcomm/records-of-comments/record-of-comments-deac-recommendations.pdf. While BIS has not implemented these proposed changes, these concepts have been raised again in the context of the export reform initiative that began in 2010.

2.2. DEEMED EXPORT ENFORCEMENT. Enforcement is carried out by BIS Office of Export Enforcement agents 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 also reported in its 2009-2012 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.

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 the PRC. 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 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 were just under $10,000 per violation. Another case was settled in October 2008 with Maxim Integrated Products, Inc. involving both unlicensed hardware exports and reexports , as well as deemed export charges involving a Chinese and an Iranian employee, iwith an extra count for releasing technology to the Chinese national while a deemed export license application was pending. The average penalty amount was approximately $5,600. An administrative case settled with ArvinMeritor, Inc. in March 2011 involving one deemed export violation, eleven violations for technical data exports, and two hardware exports . The deemed export counts appeared unrelated to the other violations, suggesting they were discovered during an internal investigation of the hardware shipment. The average penalty 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 2013 conference on technology controls, among others. 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 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 travel outside the U.S. In recent years, BIS and DoD have requested even more detailed information, such as the source of funding for an employee's education, past military service, and additional data about family members. 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 (http://www.bis.doc.gov/index.php/policy-guidance/deemed-exports /) guidance on how to prepare foreign national license applications and also other guidance concerning the deemed export rule.

3. 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 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 incremental changes to export controls on products with cryptographic functions over many years. Prior to 1996, the ITAR controlled virtually all encryption items except 40-bit key lengths and some very limited purpose encryption functions (*e.g.*, password protection, access control, authentication, fixed algorithms, and money and banking specific encryption functions). The State and Commerce Departments transferred commercial cryptography to EAR jurisdiction in December 1996, but made exceptions wherever the EAR is different, causing some to dub the encryption provisions of the EARa "Virtual ITAR" within the EAR. Nearly annual policy changes have included the proposed "Clipper Chip," a policy favoring Key Escrow techniques that failed, a policy to allow exports of 56-bit encryption items based on promises to develop Key Recovery products (which also failed), a policy allowing freer exports to favored sectors such as U.S. subsidiaries, banks, and health and medical entities, creation of License Exception ENC with different rules for Retail and Non-Retail products, liberalization of exports to the European Union, liberalization of "Mass Market" products on a basis slightly and confusingly different from "retail", and more.

This section summarizes the 2010 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.

3.1 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) implemented the Obama Administration's March 11, 2010, promise to replace

(1.1) prior product by product classification requirements (that had a 30 day wait) for most mass market and most ENC-Unrestricted ("ENC-U") items, and
(1.2) semi-annual export sales reporting requirements for most ENC-U products with
(2.1) registration of companies producing encryption items, and
(2.2) annual report by registrants of new or changed encryption products .

The rule also implemented the December 2009 Wassenaar Arrangement agreed-upon Note 4 to CCL Category 5, Part 2, to exclude from encryption controls items that do not have principal purpose of computing; sending, receiving, or storing data; networking; or information security, and where the cryptographic functions are limited to the specific functions of the item). Qualifying items are classified on the CCL based on their non-cryptographic characteristics, and can often be EAR99.

BIS published another regulation on January 7, 2011 that removed all "published" mass market and TSU eligible encryption software from EAR jurisdiction. See Part 3.3.7 below for additional detail.

While the June 25, 2010 rule did not provide most encryption reform changes for which industry has been clamoring during the past decade, the Administration promised in the Federal Register preamble and BIS press statements that this is the first step and that it is seriously working with exporters to truly streamline and clarify the current cumbersome and overly complex encryption controls. Technical advisory committees and industry trade associations are pressing now for further meaningful reform.

While the 2010 restructuring did remove controls on many items, and substituted an arguably more self-driven process, industry has long been asking to eliminate additional restrictions, such as tight controls 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 all controls on publicly available software, and to increase ENC-R thresholds, such as encryption throughput, based on foreign availability[5]. Current "controls" on products with encryption functions are more of an information gathering tool 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 new rule, focusing mostly on what more was needed, including a proposed new outline of encryption controls.

The U.S. Government has led negotiations to amend Wassenaar rules to treat hardware and software components for mass market items as mass market qualifying themselves, which resulted in an agreement at the Wassenaar 2012 plenary to allow Mass Market treatment for existing hardware components (and associated firmware) intended for use in Mass Market end-items, although not for Mass Market software components. The changes Note 3 were implemented by BIS on June 20, 2013. 78 *Fed. Reg.* 37372 (Jun. 20, 2013). Hopefully, software components for mass market items will receive similar treatment at the December 2013 Wassenaar Plenary meeting. Other issues remain under discussion.

3.1.1 <u>Overview of Review and Reporting Streamlining for Most ENC-U and Mass Market Products</u>. The 2010 changes moved exporters closer to the full standard of self classification for qualifying most 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. 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 applications, and there should be less need for second guessing by BIS/NSA of whether most products are classified 5X992 mass market with no reporting versus 5X002 ENC-U with no reporting since 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 classifications in the past. (The number of classification requests dropped from late 2010 through 2011, but have increased to almost the same levels as before the rule by July 2012.)

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

(a)(1) for exports without BIS prior 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 BIS prior 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 (only) and receipt of an Encryption Registration Number ("ERN") via SNAP filing, plus end of year reporting of self classification of all such products in spreadsheet format with some details on encryption functions, but not the level of detail required by Supplement 6 to Part 740 (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 every six month 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 application and 30 day wait prior to export and every six month 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 newly 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.

(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 foreign 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 as it has 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 self-classified and 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. This also includes mass market eligible hardware components, even after the revisions to Note 3 in June 2013. Items described in 740.17(b)(2) still do not qualify in the United States for mass market, 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 for any product, just as with other ECCNs. Exporters just are not required to do so for the new 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 (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, as described further below.

3.1.2 Ancillary Note 4 Implementation. 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 to and ancillary to the primary purpose of such products (e.g., LCD TVs, games and gaming, etc. which might use cryptography to support secondary features). The U.S. persuaded Wassenaar members to decontrol such products altogether via Note 4 to Commerce Control List Category 5, Part 2, adopted at the Wassenaar plenary meeting in December 2009. Exporters can now self-determine eligibility for Note 4, which removes from Category 5, Part 2, products that (a) do not have the primary function of computing; sending, receiving, or storing information; ; networking; or information security if (b) the cryptographic functionality is limited to supporting their other primary functions. Rather than being decontrolled to 5X002/ENC-Unrestricted 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 will need to review the rest of the CCL to determine what ECCNs apply. If no other ECCN applies, the classification is EAR99.

The preamble of the June 25, 2010 Federal Register notice includes at pages 36487-88 examples of qualifying products that had been part of the former definition of "ancillary" in EAR Part 772 and BIS presentations.[6] We think these examples should be included in the EAR itself, either in a new commodity interpretation (EAR Part 770) or in Supplement No. 3 to EAR Part 774, Statement of Understanding, which addresses Note 4. BIS has promised at least to make them available on its web site, and some are now in Frequently Asked Questions. 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. Of course, exporters can seek a formal BIS classification to confirm Note 4 eligibility, but are not required to do so.

3.1.3 Benefits and Drawbacks of the New Streamlining Rule. This is the first major substantive change to encryption regulations since 2002. For most ENC-U and mass market items, you can do a simple export registration, self classify products throughout the year, and do a report on the self classifications at the end of the year. The changes will 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 items 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 (FTC) countries 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 do 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), software with open cryptographic interfaces, among others. So, statements by Kevin Wolf, Assistant Secretary for Export Administration, and others that this is 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 See BIS's excellent guidance, including transition rules, at http://www.bis.doc.gov/index.php/policy-guidance/encryption.

As a follow-up to the 2010 changes, on January 7, 2011, BIS issued a final rule removing from the scope of the EAR: (i) publicly available mass market encryption software in object code with a symmetric key length greater than 64-bits, and (ii) publicly available encryption software in object code classified under ECCN 5D002 when the corresponding open source code meets the criteria specified under License Exception TSU (EAR 740.13(e)). 76 *Fed. Reg.* 1059 (Jan. 7, 2011). *See* discussion in 3.3.7 below.

3.2. STRUCTURE OF REVISED ENCRYPTION CONTROLS. Encryption controls are set forth principally in the following sections of the EAR:

> Part 774, Supp. 1, Commerce Control List ("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 NLR to all countries except Embargoed Countries. Some items employing encryption are excluded from control because their primary function is not for information security, and can be controlled under other CCL Categories, or even be EAR99 items.
>
> Part 742.15 sets out the roadmap for decontrolled mass market and non-mass market encryption items, License Exception availability, self-classification availability, 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.

Part 740.17, 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 the Commerce Department. 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 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.

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

Part 740, 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).

Part 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.

Part 734.2(b)(9) has a special definition of "export" for 5X002 Encryption Items, with safe harbor provisions allowing posting of ENC-Restricted 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, 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."

3.3. 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 moves to the most restrictive. Exporters of encryption products should take the following steps to determine how encryption controls apply to particular products:

3.3.1 Determine Whether You Have Encryption Eligible for Medical Note.

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. You would need to review the rest of the CCL to determine which controls apply; however, almost all items specially designed for medical end-use are classified as EAR99 by the "medical note" in Supp. No. 3 to EAR § 774.

3.3.2 Determine Whether You Have Encryption Eligible for Note 4 to CCL Category 5, Part 2 (formerly "Ancillary"). As discussed in Part 3.1.2 above, items that use encryption but whose primary function is not computing; networking; sending, receiving, or storing information; or information security are excluded from control under Category 5, Part 2. The July 25, 2010, Federal Register notice also contains examples of types of products that qualify for Note 4 in the preamble (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, 36487-88.) Note 4 eligibility is driven by the product's primary functionality, not by how or what encryption is used. Exporters can self-determine Note 4 eligibility or can seek a BIS classification ruling . 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, digital rights management, and copy protection/license management are eligible for Note 4. Such items were formerly decontrolled to 5D992 under 5A002 Related Controls notes, but are now excluded from Category 5, Part 2.

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.

3.3.3. 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, all mass market items using only up to 64-bit symmetric algorithms are self-classifiable as 5X992. See EAR § 742.15(b).

Self-classification of Mass Market items as 5X992 is permitted if the items qualify under exemptions for "short range wireless" or "personal area network" 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, and 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 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 the specific provisions of these exemptions carefully to determine eiligibility. To qualify, all cryptographic functions must fall under an exempt category. If the 5X992 decontrol classification is ambiguous, consider a formal BIS classification.

Note: Even if a product is not subject to EI controls, 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 presumptively subjects items 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.

3.3.4 Foreign Products Incorporating U.S. Encryption. Foreign products that incorporate U.S.-origin encryption components qualified for export can themselves qualify for reexport under ENC without prior review or Encryption Registration Number. This includes foreign-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 who 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.

3.3.5 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 conditions.

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

Category 5, Part 2 also provides guidance on the criteria considered to determine mass market eligibility for end-items:

> ***Note to the Cryptography Note:***
> *1. To meet paragraph a. of Note 3, all of the following must apply:*
> *a. The item is of potential interest to a wide range of individuals and businesses; and*
> *b. The price and information about the main functionality of the item are available before purchase without the need to consult the vendor or supplier.*
>
> *2. In determining eligibility of paragraph a. of Note 3, BIS may take into account relevant factors such as quantity, price, required technical skill, existing sales channels, typical customers, typical use or any exclusionary practices of the supplier.*

EAR § 742.15(b)(6) further 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-Unrestricted items to the Favorable Treatment Countries ("FTCs")[7] 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.

Until the 2013 implementation of changes to Note 3, BIS took 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. Now, existing hardware components (and related firmware) that were formerly ineligible for mass market under this policy can qualify for mass market, subject to a prior review requirement. The June 20, 2013 rule added a new paragraph b to Note 3, making the following items eligible for mass market treatment:

> ***b***. *Hardware components of existing items described in paragraph a. of this Note, that have been designed for these existing items, meeting all of the following:*
>
> ***1***. *"Information security" is not the primary function or set of functions of the component;*
>
> ***2***. *The component does not change any cryptographic functionality of the existing items, or add new cryptographic functionality to the existing items;*
>
> ***3***. *The feature set of the component is fixed and is not designed or modified to customer specification; and*
>
> ***4***. *When necessary, as determined by the appropriate authority in the exporter's country, details of the component and relevant end-items are accessible and will be provided to the authority upon request, in order to ascertain compliance with conditions described above.*

Such items still require a prior classification review, as they would fall into 742.15(b)(3), which covers chipsets and similar components.

Getting a mass market classification from another Wassenaar Member country can help given that products would otherwise be classified under different ECCNs (5X002 U.S. and no ECCN elsewhere) by different member countries.

3.3.6 <u>5X002 Items - Exports to U.S./FTC Subsidiaries</u>. 5X002 items can be exported under ENC without obtaining an ERN or filing a classification request if (a) they are for the internal use of a foreign 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 foreign national employees, independent contractors, and interns employed by such companies, except for Embargoed Country nationals.

3.3.7 <u>5D002 Items - Publicly Available Source and Object Code</u>. 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 until January 2011 deemed all them subject to EAR jurisdiction. Now, just some of them are.

On January 7, 2011, BIS issued a final rule removing from the scope of the EAR: (i) publicly available mass market encryption software in object code with a symmetric key length greater than 64-bits, and (ii) publicly available encryption software in object code classified under ECCN 5D002 when the corresponding open source code meets the criteria specified under License Exception TSU (EAR 740.13(e)). 76 *Fed. Reg.* 1059 (Jan. 7, 2011).

Publicly available software, other than encryption software, was already outside of the scope of the EAR, but certain publicly available encryption software had remained subject to the EAR 1996, when commercial items with encryption functionality were initially transferred from the jurisdiction of the ITAR to the EAR. Because there are no regulatory restrictions on making such software "publicly available" in the first place (that is, making encryption software publicly available by posting it on the Internet where it may be downloaded by anyone does not establish "knowledge" of a prohibited export under the EAR), and because, once it is "publicly available", by definition, it is available for download without restriction, BIS finally decided to recognize the obvious and remove these items from the jurisdiction of the EAR altogether, with the exception of open source code.

This rule was driven in large part by OFAC General Licenses created in March 2010 to allow exports of publicly available encryption controlled software for personal communications for Iran, Sudan, and Cuba. These changes were intended to legalize exports of such software in response to the use of social media products, such a Twitter, Facebook, Windows Live applications, and video sharing sites by protesters in Iran.

To be outside the scope of the EAR, the publicly available object code software must have been either:

- Determined by BIS to be mass market , pursuant to EAR §742.15(b)(3), or
- Self-classified as mass market eligible; or
- Qualified for License Exception TSU (notification by e-mail of the url is sufficient) as described below.

However, before you may self-classify encryption software as mass market, you must first submit an encryption registration with BIS, and you must subsequently submit an annual self-classification report listing items self-classified during the year, or request a classification from BIS. So, unless the software has been classified by BIS, or has been self-classified and will timely appear in a self-classification report to BIS, or qualifies for TSU for open source software, it is still subject to the EAR even when made publicly available.

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. Exporters were unclear whether the January 2011 clearly released free patches and updates that can only be used with proprietary products (one can certainly argue that point, and it appears that most patch providers do not screen their downloads in practice, but they were only useful for the product being patched/updated); however, BIS personnel have given such free updates or drivers as examples of qualifying "freeware."

This rule is a welcome, long awaited development that makes the EAR more consistent with the OFAC sanctions' treatment of publicly available software, which is a goal of export reform. This author also believes that the revisions remove the impediment to treating such publicly available software as "informational materials" under the so-called Berman Amendment to the Trading with the Enemy Act and the International Emergency Economic Powers Act because they are no longer "subject to the EAR."

Items that are not eligible for release from EAR jurisdiction are still 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 non-publicly available source code. TSU also does not authorize exports of proprietary software containing only open source encryption components such as OpenSSL, which often surprises exporters.

If you qualify for TSU, you need not provide updates if you elect to provide the Internet location rather than providing disks. Section 740.13(e) purports to restrict knowing exports 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 4.3.6 below on new Treasury Department General Licenses for free and anonymous software exports to embargoed countries and BIS' advisory on same.)

3.3.8 <u>5X002 Items Not Listed in 740.17(b)(2) or (b)(3) qualify for (b)(1)</u>. 5X002 items other than those listed in 740.17(b)(2) or (b)(3) can be self-classified and determined to be eligible for ENC-Unrestricted if the exporter or manufacturer has obtained an ERN and complies with the annual self classified product report requirement described above and below. 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-Unrestricted to any end-user, except to Embargoed Countries.

3.3.9 <u>5X002 Items - 740.17(b)(2) and (b)(3) Items</u>. Items listed in 740.17(b)(2) ("ENC-Restricted") and 740.17(b)(3) ("ENC-Unrestricted") 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-Restricted items, particularly cryptanalytic items, are also subject to distribution restrictions to government end-users within the FTC. ENC-Restricted 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-Unrestricted items under (b)(3) may be exported to all end-users in all but E:1 countries.

3.3.10 <u>5X002 Items - ENC Ineligible - License Required</u>. A few items and situations are not eligible for License Exception ENC use, and a license is required:

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

3.3.11 Mechanics of New Encryption Structure. We summarize below the key requirements, but it is worthwhile to review the extensive BIS guidance at: http://www.bis.doc.gov/index.php/policy-guidance/encryption.

3.3.11.1 Obtaining an Encryption Registration Number ("ERN"). A prerequisite to self-classification of eligible ENC-U items under 740.17(b)(1) or Mass Market under 742.15(b)(1) is obtaining an ERN. An ERN is also required for filing a required classification request. The process of obtaining one is fairly simple. SNAP-R 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 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 a PDF 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.

3.3.11.2 Annual "Self-Classification" Report. The other prerequisite to self-classification and eligibility for ENC under 740.17(b)(1) or Mass Market under 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 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 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 740.17(b)(1) and 742.15(b)(1) items.

3.3.11.3 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 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 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 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 740.17(b)(2) and 740.17(b)(3) items, the second for 742.15(b)(3), and the third option for any other encryption items submitted for review.

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

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.

3.3.11.4. Semi-Annual Shipment Reporting Requirements for 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 740.17(b)(2) ENC-Restricted items and 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 (though Microsoft will not be held to the accuracy of the many "Bill Gates" or "Darth Vader" registrations that it reports). 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.

The 2000 and 2004 encryption changes exempted from reporting short range wireless, client Internet appliances, client wireless LAN cards, ENC-Unrestricted 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 underscored that reexports (other than from Canada) need not be reported. The October 3, 2008, revisions 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 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 say they will still consider such requests.

3.3.11.5. 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 foreign 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 740.17(b)(2) ENC-Restricted and 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).

3.3.11.6. ENC Compliance Tips. Exporters need to take appropriate steps to make sure that they do not ship ENC-Restricted 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-Restricted 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-Restricted encryption products under this provision on the Internet, with warnings as to Know Your Customer Guidelines and avoiding violating the other 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. We have a number of model compliance clauses.

3.3.11.7. Commercial Source Code That Is Not Publicly Available. EAR § 740.17(b)(2) provide that proprietary encryption source code not publicly available pursuant to EAR § 740.13(e)(License Exception TSU) will qualify as ENC-Restricted, 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.

3.3.11.8. Open Cryptographic Interfaces. Items incorporating an Open Cryptographic Interface may be exported under License Exception ENC Restricted 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 R&D use, but otherwise require a license.[8] 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 ELAs for products with OCIs, and approved Microsoft Vista for mass market treatment only after other countries did so when BIS/NSA had only approved it under a curious letter authorization for a year or so.

3.3.11.9. Reexports of Resultant Foreign-Produced Products and the "Crypto-Aware" Concept. Foreign 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). This provision was amended in the October 3, 2008, rule to add a sentence clarifying that such foreign 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? 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 be the direct product of U.S.-origin NS controlled technology for the non-U.S.-origin items to be subject to the EAR).

The scope of this statement is not entirely clear, but seems to reflect an increasingly conservative BIS interpretation in recent years of the applicability of ENC review requirements to items that do not themselves incorporate encryption functions or 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 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 as sufficient to. 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.

BIS personnel later changed this interpretation through statements at conferences, as well as to us in the context of classification reviews, where they have said 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 ENC or mass market review procedures. This may be a reasonable interpretation, but it is nonetheless 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 foreign products that have no actual U.S. content and thus are not subject to the EAR pursuant to Parts 734 and 736.

3.3.12. Encryption Licensing Arrangements (ELAs) and Other Licenses. The regulations continue to provide that encryption licensing arrangements will be favorably considered for exports to governments or ISPs and telecoms for services to governments specific to civil government end-users. Expect to see certain governments excluded upon case by case review. In the June 25, 2010 rule, 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.

3.4. CONCERNS REMAIN RE "HIDDEN" LICENSING REQUIREMENTS FOR OFFSHORE DEVELOPMENT AND SALES OF ENCRYPTION ITEMS. One of the more difficult encryption provisions had been former EAR § 744.9, which prohibited technical assistance, including training, intended to aid a foreign 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, OEE has not enforced this provision to our 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 did 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 which 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" is provided only obliquely in ENC and mass market encryption regulations, as the regulations do not spell out 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 it were spelled out.) The rule, long in advisories, allows exports of software or hardware without being subject to strict "EI" controls if access control encryption functions (decontrolled to 5D992) prevent a user from gaining access to the crypto functions without a key; but, the exporter using the policy 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, self-classifiable under the provisions of 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 control the keys effectively, as that is often harder to do. If you treat 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.

3.5. 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, rule replaced EAR § 770.2(n) with reworded notes, now found in 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 new note adds language that says 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 is very helpful, since such changes can include new algorithms or upgrades, but BIS reviews them all the time. The notes otherwise reinforce their interpretation that version changes do not require a new classification review, as long as the changes are not relevant to the cryptographic functionality of the product that was reviewed (*i.e.*, do not affect the Supplement 6 information). This is consistent with the long standing BIS interpretation of subsequent bundling, but the new wording and explanations of some at BIS may cause some to conclude that there is a difference in interpretation, which is difficult to discern.

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.

3.6. 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 quite high with large volume exports. While it is inevitable that ENC-Restricted 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 web sites 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 foreign nationals and persons outside the United States.

3.7. FURTHER CHANGES NEEDED. The RPTAC 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-Unrestricted categories, so as to eliminate wasted effort distinguishing among the three categories, and removing more of the "virtual ITAR" control vestiges, including as described further in 4.3.6 below treating all freely available encryption software as not subject to the EAR whether or not in object code. While the October 2008 and June 2010 regulations 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, BIS has solicited input from industry about how to structure encryption export controls based on a "green field". TechAmerica and others 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://beta-efoia.bis.doc.gov/index.php/component/docman/doc_view/696-license-exception-enc?Itemid=526.

4. CHALLENGES FOR EXPORT MANAGERS IN AN E-COMMERCE OR CLOUD ENVIRONMENT

More and more, exporting like other modern business activities occurs in a partly to fully automated environment. Export compliance software programs are helping exporters to facilitate compliance. Automating exports of software and technology, among other things, first via what was called "e-commerce" and more recently the cloud present new and unique challenges to exporters. For example, if only the computer "knows," do the "Know Your Customer" guidelines apply?

4.1. WHAT IS E-COMMERCE" FOR EXPORT CONTROL PURPOSES? The first question to address in applying export compliance to e-commerce activities is what do we mean by the terms e-commerce, e-business, B2B, and similar means of automated commerce for purposes of this discussion? These buzz words mean different things to different people and different parts of the same business. For example, taking orders over the Internet, but shipping manually is one form of e-commerce, but exporters can employ the same export compliance procedures at the shipping end as they do with all other export shipments. It can also apply to posting developer information and other activities besides buying and selling. This discussion will address fully

automated software downloads where there is no human involvement in most transactions. What we learn from this can be applied to order taking functions for hardware and many other B2B functions. We will then briefly address "cloud computing."

4.2. LIMITED EAR PROVISIONS ADDRESSING E-COMMERCE. The EAR addresses e-commerce only in three places. First, EAR § 734.2(b)(9) defines as an export, for "EI controlled" encryption source and object code only, making such software available for download. The EAR does not define making available other software for download as an export. Nevertheless, could it be aiding and abetting an illegal export if the company has records that customer downloads were from Cuba or another country not eligible to receive such an export? The law is not clear in this area, and gray areas of the law make exporters uncomfortable. Second, the Census Foreign Trade Statistics Regulations in 15 C.F.R. § 30.55(o) as of July 10, 2000 thankfully clarifies longstanding policy that intangible exports (via e-mail, downloads, and other electronic transfers) do not require exporters to file Shipper's Export Declarations or AES electronic filings. Third, EAR § 740.13(e)(4) states for publicly available encryption software that "[p]osting of the source code or corresponding object code on the Internet . . . where it may be downloaded by anyone would not establish 'knowledge' of a prohibited export or reexport . . . . In addition, such posting would not trigger 'red flags' necessitating the affirmative duty to inquire under the 'Know Your Customer' guidance . . . ." Preamble language to the January 2000 encryption regulation implementing that section applied the same language to License Exception ENC Unrestricted eligible software, and similar preamble language to the June 6, 2002 regulations similarly did for mass market software.

It is helpful to apply the regulations where they do apply, then use that knowledge to determine what types of compliance techniques make sense for other types of software.

4.3. APPLICATION OF EAR TO CERTAIN TYPES OF SOFTWARE E-COMMERCE.

4.3.1. ENC Restricted Encryption Software. EAR § 734.2(b)(9)(ii) states that the export of source code and object code software controlled for "EI" reasons under ECCN 5D002 (except public source and community source) includes downloading, or causing downloading to locations outside the U.S., or making such software available for transfer outside the U.S. over communications facilities accessible to persons outside the U.S., including bulletin boards, ftp and www sites, unless the person takes "precautions adequate to prevent unauthorized transfer of such code." Adequate precautions for web sites are described in EAR § 734.2(b)(9)(iii) only for "ENC-Restricted" 740.17(b)(2) Encryption Items, certain encryption source code, and encryption toolkits as, subject to the general prohibitions described in EAR Part 736 (e.g., not to Embargoed Countries, Denied Persons List, or knowingly to/for proliferation end-users or uses), including such measures as:

A. The access control system, either through automated means or human intervention, checks the address of every system outside of the U.S. or Canada requesting or receiving a transfer and verifies such systems do not have a domain name or Internet address of a foreign government end-user (e.g. ".gov," ".gouv," ".mil" or similar addresses);

B. The access control system provides every requesting or receiving party with notice that the transfer includes or would include cryptographic software subject to

export controls under the EAR, and anyone receiving such a transfer cannot export the software without a license or other authorization; and

C. Every party requesting or receiving a transfer of such software must acknowledge affirmatively that the software is not intended for use by a government end-user, as defined in part 772, and he or she understands the cryptographic software is subject to export controls under the export administration regulations and anyone receiving the transfer cannot export the software without a license or other authorization. BIS will consider acknowledgments in electronic form provided they are adequate to assure legal undertakings similar to written acknowledgments.

Not required by the regulations, but wise for exporters to consider as long as one is obtaining an acknowledgment, are assurances that the item will not be used by or for any nuclear, chemical or biological weapons, or missile end-user or use, or a denied party or entity, and that the recipient takes responsibility for import and use controls in destination. One should also ensure that the acknowledgment is given before downloading can occur.

Many exporters also at least consider employing some form of screening against Denied Persons and Entity List recipients, Specially Designated Nationals, etc., and country suffixes (*e.g.*, for T-5 countries). Most systems do not do this well. They make sure the system kicks out close calls for human review.

4.3.2. Public Source and Object Code EI Encryption Software. As discussed above in Section 3.3.7, certain publicly available mass market software and object code derived from published source code is not subject to the EAR, but U.S.-origin open source code and proprietary software incorporating open source and other "freeware" remain subject to the regulations. EAR § 740.13(e) states that ECCN 5D002 encryption source code and object code that qualifies as publicly available under EAR § 734.3(b)(3) and is not subject to an express agreement for the payment of a licensing fee for any product developed with [it] is released from "EI" controls. Ordinarily, publication should mean that such software is outside the scope of the EAR, but the provisions go on to state that such software may be exported or reexported without review under License Exception TSU, provided one has submitted written notification to BIS and NSA.

The License Exception also states that one may not knowingly export it to the T-5 countries. But, it helpfully states that posting of the code where it may be downloaded by anyone would not establish "knowledge" of a prohibited export or posting would not trigger "red flags" necessitating the affirmative duty to inquire under the "Know Your Customer" guidance provided in Supp. No. 3 to EAR Part 732. The special "export" definition for encryption software (including posting to the Internet) in EAR § 734.2(b)(9) excludes public source and community source. EAR § 740.17(a)(5)(i). Thus, no screening at all for publicly available software, including but not limited to encryption software, is warranted. Some exporters apply the same types of screening as described above for ENC-Restricted items to some such software just because it is easier to employ one model for all software. That is not necessary, though. A BIS Advisory Opinion dated September 11, 2009, confirmed this.

4.3.3. ENC Unrestricted Eligible Encryption Software EAR § 740.17(b)(1), (3), and (4). The regulations cease to provide much guidance in this area. It is not excluded from the special definition of "export" like public source and community source. This exclusion was a last minute change to the January 14, 2000 regulations. On the other hand, the EAR also impose no specific screening requirements in EAR § 734.2(b)(9)(iii) like those for ENC-Restricted EI software. The preamble to 65 *Fed. Reg.* 2492-93 (Jan. 14, 2000) (and certain other amendments) twice says what was then called retail encryption software is exempt from Internet download screening requirements, but it also says "other general prohibitions apply." This leaves the law a fuzzy gray area. Most export practitioners who have studied the area have concluded that:

A. For anonymous downloads (no information is collected on the customer), they should have automated screens against Embargoed Countries, "reverse Domain Name Search" to avoid strict liability if records are maintained for destinations.

B. When one does have customer data, records, etc., there is no clear duty to screen, but it may be wise to screen against Denied Party List, Entity List, Specially Designated Nationals, etc. to avoid likely strict liability. This is hard and not many exporters have been doing this over the years, though more and more do so for encryption software.

C. There is no duty to screen for proliferation risks, and there is not much risk if the product cannot be directly employed in such activities, but many screen sensitive products or at least get certifications from the end-user.

4.3.4. License Exception TSR Eligible Software EAR § 740.6. Posting such software to the web is not defined as an export, but what about records, especially when one obtains payment and customer data before they can download? This could be a fascinating legal case as to whether an export by the poster exists or there is "aiding and abetting". (Downloading by the customer seems clearly to be an export.) We and other lawyers will "defend" anyone who asks, but many would just as soon pass on that privilege. Before one may lawfully export License Exception TSR software, one must obtain prior written assurance (if this is an export). Thus, it seems wise to screen such items similar to the model above for ENC Unrestricted encryption software.

4.3.5. NLR and License Exception TSU Eligible Software (EAR § 740.13 Mass Market, Non-EI beta TMP, NLR Based on CCL Classification, EAR99 Items). Again, if not encryption items, posting to the web is not defined as an export, making this another "fascinating legal case" if the company has records. Again, it seems wise to screen such items along the same model as ENC-Unrestricted items if downloads are not anonymous. In particular, for mass market encryption software as described above, the Preamble to BIS's June 6, 2002 regulation stated:

> All existing restrictions and licensing requirements to embargoed or designated terrorist supporting countries (Cuba, Iran, Iraq, North Korea, Sudan and Syria) and sanctioned persons are continued by this amendment. Posting of mass market encryption software on the Internet (e.g., FTP or World Wide Web site) where it may be downloaded by

> anyone would not establish 'knowledge' of a prohibited export or reexport. In addition, such posting would not trigger 'red flags' necessitating the affirmative duty to inquire under the 'Know Your Customer' guidance provided in Supplement No. 3 to part 732 of the EAR.

In substance, this is the same as language in EAR §§ 740.13(e)(4) & (6) for License Exception TSU (discussed above in subsection for Public Source and Object Code EI Encryption Software). However, in the case of mass market encryption, this limited safe harbor is in the Preamble, not the regulations. As discussed above in the subsection for ENC Unrestricted encryption software, that was also the case for "retail" products in the January 2000 regulation, so the placement of this provision may justify those who have not been screening downloads. Still, we have usually advised that exporters who have records of downloads into these countries may want to consider automated screening (e.g., "Reverse DNS") to avoid such downloads to embargoed countries because it would seem that enforcement officials could argue that they otherwise "know" of such prohibited exports. As stated above, you probably do not wish to do that for "freeware" based on the following.

4.3.6 OFAC General Licenses and Commerce Advisory and Proposed Regulation for Published Software. In March 2010, the Office of Foreign Assets Control ("OFAC") of the Treasury Department amended 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 that 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 (effective March 8, but published March 10, 2010). That OFAC regulation was issued pursuant to a December 15, 2010 notification by the State Department to Congress that it was in the national interest to waive restrictions of the Iran-Iraq Arms Non-Proliferation Act of 1992 (Pub. L. 102–484) (50 U.S.C. 1701 note) (''IIANPA'') and section 6 of Executive Order 13059 of August 19, 1997 (''Prohibiting Certain Transactions With Respect to Iran'') because certain software and services that enable personal communications and other sharing of information over the Internet are controlled by the CCL because of their encryption functionality. The exclusion of "published" software from the EAR by EAR 734.7 specifically does not include software classified under ECCN 5D002 and at the time did not include mass market ECCN 5D992 classified encryption software, so they are/were controlled under the CCL and thus cannot 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."

BIS ultimately issued a final rule in January 2011 releasing certain publicly available encryption object code software from EAR jurisdiction, subject to compliance with notice requirements for TSU or requirements to qualify encryption mass market software (see Section 3.3.7 above), which removed some of the issues relating to limits on downloads.

In the meantime, in a September 11, 2009, BIS Advisory Opinion, BIS stated that, in certain circumstances, an exporter posting software with encryption functionality on the web for free download would not be in violation if such software is downloaded to an embargoed country without the company's knowledge. Our firm obtained a refined version of this "don't ask, don't tell" advisory for a client that fits more common fact patterns. Exporters who post such free downloads probably do not want to screen against embargoed country users anymore for such products, though that is a fact specific determination that each company will want to make product by product, and many find one method of screening for everything easier to administer. We likewise have obtained similar guidance from OFAC regarding its regulatory restriction that the new General Licenses are not available if the exporter "knows" such software is being exported to the Governments of Iran, Sudan, or Cuba, respectively. The January 2011 rule change eliminates many of these issues by releasing some publicly available encryption items from EAR jurisdiction.

Note that free patches and updates that can only be used with proprietary products for customers do not clearly qualify as publicly available, although one can certainly argue that point, and it appears that most patch providers do not screen their downloads in practice. As stated earlier, some in BIS have recently been advising that free patches and drivers do qualify as publicly available.

4.3.6. Licensable Software. In most cases, software that would require a license for export to many countries would not be a good candidate to allow for automated downloads. But, recall that electronic transfers of licensed exports are lawful and do not need an AES filing. Many companies do export electronically technology and software that is covered by a license. To do so, it is wise either to set up a closed system or some form of access control to ensure that all such exports are made within the scope of the license and that the compliance procedures are documented. Exporters should avoid giving carte blanche to those without experience to make judgments. Many exporters employing electronic export procedures for ITAR and other licensed software put together Guidance memos describing procedures and precautions being employed.

4.4. WHAT TYPES OF EXPORT COMPLIANCE PROCEDURES ARE REASONABLE AND SUFFICIENT FOR DIFFERENT PRODUCTS? Remember, that export screening may be wise, but it is not legally required. In other words, export compliance in this area, like others, is a matter of business judgment as to what is appropriate risk management. How much due diligence is appropriate for e-commerce export compliance depends on the nature of the violations one is seeking to avoid, and that can depend on the nature of one's products. As previously described, "strict liability" civil violations can occur from exporting without a license required by the product classification, and probably exporting to a denied party, entity, or SDN if one has "knowledge" of the entity name because the law gives exporters "constructive knowledge" based on publication of these lists in the Federal Register. "Knowledge" violations include sensitive nuclear, chemical or biological weapons, or missile end-uses or end-users, red flags of likely diversions, and a few others. Despite years of pleading by industry, the U.S. Government has never developed any positive or negative lists of items required or not required to be screened, but if an item cannot possibly be directly employed in such end-uses or by such end-users for the activities in question, some lawyers support the notion that it would not be negligent to skip EPCI screening. For more sensitive items, several companies and providers have been

developing fuzzy logic word searches to reduce the risk that of allowing automated downloads to customers whose orders and other submissions include words that might, in 20-20 hindsight be considered red flags. Exporters employing such techniques are seeking to avoid the interesting case of whether OEE could prove "knowledge" based only on computer records without proving that any human knew. Most lawyers think that certifications are easy to include, either in click wrap license agreements or separately, even if such self serving statements many not always be sufficient.

4.5. PRACTICAL CONTROLS ON EXPORTS OF TECHNOLOGY AND SOFTWARE – SERVER ACCESS. One of the most demanding export compliance challenges is how to control access to server data and source code in a modern international environment. The business model encourages world wide collaboration among research and development engineers, but the regulatory model inhibits it.

Export compliance officials faced with questions of whether exports have occurred of sensitive technology or source code would prefer to be able to prove that non-U.S. persons or locations that were not allowed to access data did not in fact have access. BIS officials have not said whether enforcement has to prove that technology was in fact read or downloaded versus merely accessible. DDTC has clearly taken the position that access equals an export. We believe that the better position is that the government must prove an actual export across borders or a deemed export of the data or source code to a foreign national in the United States to make out an enforcement case. Nevertheless, the only practical export compliance steps that a company can take beyond education is to limit access to export controlled data and source code based on passwords, rights in certain areas, and other mechanisms. Such technology transfer control plans can also nip such an enforcement investigation in the bud more readily than telling the agents they have to prove the violation.

Controls on exports of software by automated download and server access requires that the export compliance personnel bring their chief information officer and security officer, or at least the IT department, into the export compliance program. This cannot be controlled like other exports at the order entry level. This requires classifying, at least on a broad brush basis, the software and technology that is available, and setting up mechanisms to restrict availability until there are licenses obtained or a review mechanism can be applied. Exporters should also beware not just of the persons with a need to know who have access but also of the super users in the IT department who have access, but really are unlikely to be interested in content so much as in the process. State and Defense personnel currently audit for such access for government contractors with facility security clearances.

Questions to ask include:

- What controlled software or technology is on a given server?
- What servers should be dedicated to export controlled software and technology?
- Who will classify and determine jurisdiction for technology and software?
- Will you control access at the file level, at the user level, at the domain level, or otherwise?
- Should you have separate servers for export controlled technology and software?

- Should you use encryption of files? (That changes the file management challenge to a key management challenge and requires you to review the encryption mechanism exports.
- Can you prove nothing on your servers is controlled to destinations and persons with access?
- Do your strategic partners give you access to their servers, or vice versa; do those servers contain controlled data; and, do the two companies determine whether non-U.S. employees have access?

4.6. A WORD ABOUT SERVICES VERSUS DATA. Although beyond the scope of this article, exporters should be aware that, even when exporting only public domain technology or software not subject to export controls, your activities might still involve U.S.-origin services that are subject to license requirements if they are (a) "defense services subject to the ITAR or (b) services to embargoed nationals subject to OFAC administered embargoes and sanctions. The line beyond which such activities can rise to the level of prohibited "services" can be very fuzzy and subject to interpretation.

4.7. CLOUD COMPUTING.

The increase of service-based or "cloud" computing has created questions about the degree to which cloud service providers and cloud users are responsible for exports of technology and software that may take place in the context of the provision and use of such services. NIST has defined cloud computing as a model for enabling network access to a shared pool of computing resources (e.g., networks, servers, storage, applications, and services), with essential characteristics: On-demand self-service, broad network access, resource pooling, rapid elasticity, measured service (metered). See http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

This is a very broad definition, and covers many types of services, such as the following:

- Remote data storage/backup: Using a provider's storage network over the Internet for primary or backup storage of files, data, or other information.
- Software as a service (SaaS): Using a provider's applications running on a cloud infrastructure.
- Platform as a service (PaaS): Deploy onto a cloud infrastructure the user's own or third party applications created using programming languages, libraries, services, and tools supported by the provider.
- Infrastructure as a service (IaaS): Access processing, storage, networks, and other fundamental computing resources where the user can deploy and run software, which can include operating systems and applications.

The concept can cover "public" cloud services, where each user's data is not necessarily segregated from that of other users, in terms of its location and method of storage. It can also cover "private" cloud services, where the services are segregated by user, as well as hybrid public/private models. Given these differences, "cloud" computing services do not face precisely the same export compliance models, but these types of services to present similar

compliance issues. BIS has taken the lead in responding to some of the issues raised by cloud computing, while DDTC and OFAC have not yet provided comprehensive guidance. Thus, this section will focus on EAR compliance issues, then will address the additional issues raised under the ITAR and OFAC Sanctions Regulations.

4.7.1 EAR.

The common questions that arise in analyzing EAR cloud computing export compliance, regardless of the mode of delivery, are similar to a standard analysis for transfers of technology and software, but with an additional question that is frequently absent in "traditional" exports:

(1) Has an actual "export" of technology or software occurred?
(2) Has a "deemed export" of technology or software occurred?
(3) Based on classification and destination, is an export license or License Exception required to authorize any such exports?
(4) Does the cloud service provider, cloud service user, or anyone have sufficient knowledge of the classification of the items and destinations involved in such exports to be held responsible for making a license determination?

BIS has issued two advisory opinions in response to questions from cloud computing service providers, which address these questions primarily in the context of "public" cloud computing situation. The opinions can be accessed at http://www.bis.doc.gov/index.php/policy-guidance/advisory-opinions. An underlying premise of these opinions is that the provider lacks detailed knowledge about what technology and software are being placed on their systems by users – and may not even know who is using the system. It is also presumed that the user lacks detailed knowledge about the location of the provider's computing assets and the nationality of administrative personnel.

The first advisory opinion was issued on January 13, 2009, and it confirmed that exporting technology or software via a cloud solution is treated like an export of technology or software by any other means. However, the opinion does indicate that providing cloud services alone (whether providing remote storage or remote computing capacity) is not an activity that is subject to EAR, unless the provider knows that the service will assist in design, development, production, of missiles or chemical or biological weapons, which is prohibited by EAR § 744.6.

The 2009 opinion also indicates that, in the absence of an agency relationship between cloud provider and cloud user, the cloud provider is not the exporter/USPPI when a user exports data stored on the cloud or resulting from use of the cloud, because the user receives the primary benefit of an export that is effected through the cloud. Note, however, that the analysis seems to assume that the cloud user is the USPPI because the user is aware that an export is occurring. Further, it indicates that cloud providers need not inquire about the nationality of cloud users because simply providing computational capacity via the cloud is not subject to the EAR.

A second BIS advisory opinion followed on January 11, 2011, clarifying the circumstances under which deemed exports do or do not occur in cloud computing contexts. It indicated that cloud computing service providers are not required to obtain deemed export licenses for foreign national administrators who service and maintain cloud computing systems. The opinion reasoned that, because the service provider is not an "exporter," the service provider would not be making a "deemed export" if a foreign national network administrator monitored or screened user-generated technology subject to the EAR. This is limited to circumstances where the cloud provider does not monitor or screen user-generated content stored and/or shared in the cloud, except when required to do so by law, through automated tools like spam filtering or spell check, or with user consent (e.g. troubleshooting individual accounts).

Taken together, these advisories pose a scenario where technology and software may be crossing borders or be released to foreign nationals, such that "exports" are occurring, but there may not be anyone who qualifies as an "exporter," as neither the provider nor the user may have sufficient knowledge necessary to fill that role. However, users are concerned that the opinions more clearly limit liability of cloud providers, but not users as the "exporter" who do not necessarily know where they may be exporting from or to.

For example, suppose a U.S. cloud user uploads 3A001 technology into a cloud storage service, intending only to provide access to U.S. person employees in the United States. The data is placed into the cloud, and due to backups and load balancing, copies of the technology are stored permanently or temporarily in servers located in the United States, Singapore, and Israel, with administrative oversight of those servers by Indian nationals. All of this takes place without the user having any knowledge of the transfers, because the provider does not disclose to the user the location of the provider's computing assets, or if they do that, do not disclose where the data may reside at any given moment. Conversely, while the service provider may be aware that data loaded by U.S. users is automatically exported to the other servers, the provider does not inspect the items and lacks knowledge of which technology is subject to what export license requirements.

Applying the two opinions, the provider would not be the USPPI, and so would not be held responsible for export compliance. The user technically could be considered the USPPI, but may lack sufficient knowledge that the export occurred, or may not have engaged in conduct that was the proximate cause of the export, such that BIS may not be able to hold the user responsible for failing to obtain any required export license.

It is clear from the opinions that if the cloud user knows that an export or deemed export will occur through the transfer or release of software or technology, they can be held liable. For example, if a U.S. employee puts technical data into the cloud intending for it to be accessed by colleagues outside the United States, the user will be responsible for determining export compliance responsibility and obtaining any required authorizations.

Industry associations have been working with BIS to achieve further clarification, but as discussed below, are being careful what they ask for.

4.7.2 ITAR

As of the date of this writing, DDTC has not yet issued guidelines or regulations relating to the use of cloud computing resources in relation to the storage of ITAR-controlled technical data, or with respect to the provision of defense services. DDTC officials verbally have advised that the only ITAR compliant cloud is one with all servers located in the United States, administered by U.S. Persons, and accessible only by U.S. Persons. That makes for an expensive and limited use "private" or shared private cloud to be ITAR compliant, given that they also treat ability to access as sufficient to constitute an export.

DDTC did solicit the advice of the Defense Trade Advisory Group ("DTAG"), which presented a white paper and recommendations on May 9, 2013. The crux of the DTAG's recommendation was a proposal to re-define "technical data" in ITAR 120.10 to exclude information that is encrypted in conformance with a defined or referenced standard, or to provide for an exemption to licensing requirements for technical data that is appropriately encrypted. The DTAG report and recommendations can be accessed at http://www.pmddtc.state.gov/DTAG/index.html.

DDTC officials have indicated that regulations or guidance may be issued in early 2014 to address the DTAG's recommendations and other issues related to cloud computing.

We have discussed whether, in the meantime, we could defend a potential violation by arguing that if the recipient only had access to encrypted technology or software without access to cleartext, there was no export of technology or software, merely gibberish.

4.7.3 OFAC Sanctions Regulations

OFAC Sanctions Regulations present additional issues for cloud computing service providers and users, particularly due to the regulation of the export and import of services by the OFAC Iran and Sudan sanctions, as well as the proliferation of assets blocking sanctions targeted at Specially Designated Nationals (SDNs) and foreign governments.

For example, under the EAR, a U.S. person can furnish a software-as-a-service offering to an end-user in Iran without violating the EAR, assuming there is no download of U.S.-origin software required to provide the service. However, the U.S. person would be exporting a service to a person in Iran, which is prohibited by OFAC's Iran Transactions and Sanctions Regulations (ITSR). Additional ITSR prohibitions against importing services could be triggered if that person is an employee or service provider, who is using the SaaS to provide services to the U.S. person.

While not squarely addressing cloud computing in its regulations, OFAC has attempted to authorize the provision of a particular segment of cloud computing services to embargoed countries. In response to the use of social media to organize anti-government activities in Iran and other Embargoed Countries, OFAC has issued general licenses to authorize the provision of services, software, and hardware necessary to support personal communications in such countries. For example, ITSR § 560.540 and General License D (issued May 30, 2013, http://www.treasury.gov/resource-center/sanctions/Programs/Documents/iran_gld.pdf) authorize

the provision of free and paid services relating to the support of personal communications over the Internet or other means of telecommunication in Iran. General License D also authorizes sales of specified equipment, such as computers, smart phones, and similar items, necessary to carry out such personal communications. There are also restrictions that prohibit providing such services to the Government of Iran or other SDNs

The impact of these General Licenses on cloud computing seems to be primarily on free or paid "public" cloud services, such as those provided by Google, Microsoft, Apple, and other similar mass market service providers. Restrictions that require the communication to be of a personal and apparently non-commercial nature appear to inhibit the use of General License D to authorize, for example, the use of U.S-origin private cloud (aka VPN) services by a foreign business traveler while traveling in Iran, or the hosting of a website for an Iranian business. Industry is still discussing these and other issues with OFAC.

4.7.4 Practical Implications for Providers and Users

At present, due to the relatively provider-friendly BIS opinions, most "public" cloud service providers rely on representations or clauses in their terms of service to address lingering liabilities – particularly under the cloudier environment of the ITAR and OFAC Sanctions Regulations -- that may arise in providing such services. For example, many service providers permit the storage or generation of export controlled technical data in the cloud by their users, subject to representations by the user that no ITAR technical data will be generated or stored, and similar representations about not using the services in Embargoed Countries or in support of missile/WMD proliferation activities that are prohibited by EAR Part 744.

Many service providers buttress such latter assurances with IP blocking or reverse DNS screening to minimize the chance that their services will be used from embargoed countries. Due diligence procedures also vary based on the type of service provided. Free personal communication cloud services are subject to fewer restrictions, and merit a different type of due diligence than, for example, the offering of SaaS CAD software that could be used to design any type of military or dual-use article, and where more substantial support may be required from the service provider in using the software, enhancing the risk that the provider will acquire actual knowledge regarding the export control classification of the user's technical data.

Many users of cloud services who generate or store export controlled data also exercise additional due diligence, particularly the less "public" the cloud service offering is. In setting up "private" clouds, users frequently request information about the location from which the services will be provided, and the nationalities of service provider personnel who will have access. This is more common with users who have ITAR, EAR Missile Technology, or other highly export controlled technical data or software.

4.8 EXPORTERS SHOULD BE VERY CAREFUL ABOUT ASKING THE GOVERNMENT FOR MORE CLARITY IN E-COMMERCE OR CLOUD COMPUTING CONTROLS. The law in the area of e-commerce and server access is a bit fuzzy, but more clarity may not in fact make for better law. The current law allows exporters of different types of products and with different budgets to make different judgments as to what types of controls are appropriate for their company, their

products, and their e-business environment. After expending significant resources to develop a fancy electronic screening system, it will be tempting for many exporters to insist that the government require competitors to do so, too. But remember, that asking for clear, bright lines got us the "deemed export rule." Regulators tend to micromanage with technological toys, and write rules that are more specific than needed. (*See, e.g.*, EAR § 762.4, which requires exporters keeping electronic records to do so in a manner far more restrictive than originals, provisions with which not many electronic systems fully comply.) At worst case on the gray scale, the rules for e-commerce and cloud computing are the same as for other exports. For the most part, it seems wise to let best practices develop on an as-needed basis, and to ask the government for reasonable, practical improvements to the rules, such as stating that posting ENC Unrestricted, TSU NLR, and EAR99 items to the web is not an export or at least does not raise any "red flags".

5. INTERNATIONAL DEVELOPMENTS ON TECHNOLOGY CONTROLS.

The U.S. - for the entire Cold War and most of the time since then - has been the only country to apply export controls to "intangibles", technology and software transmitted electronically and not written on paper. The Australia Group and the Missile Technology Control Regime agreed in 2002 to control exports of technology in intangible form. The Wassenaar Arrangement had done so in 2001, and the EU and its members had in 2000. Thus, the transfer of technology across borders is regulated by regime partners.

However, the EU and all of these regimes, and to the best of this author's knowledge, all countries, have rejected deemed export control rule proposals, at least for dual-use technology (often after learning of the difficulties faced U.S. companies). Indeed, the robust privacy and antidiscrimination laws of the EU, Canada, and other countries tend to take precedence, as "deemed export" compliance often requires inquiries regarding the nationality, citizenship, and national origins of employees. Thus, deemed export controls remain for the most part unilateral U.S. controls for dual-use technology.

Conclusion

It is hoped that this article will help shed some light on the difficult application of export controls on technology and software. Further reforms are needed in some areas to avoid the controls simply being a trap for the unwary. Remember, though, that asking for clarity resulted in the "deemed export rule". Tight compliance programs can help reduce the complexity to speed bumps in most cases as opposed to more troublesome roadblocks.

BHF/DFO

---

[1] Partner, Berliner, Corcoran & Rowe, L.L.P., Washington D.C.; J.D., University of North Carolina at Chapel Hill School of Law 1981. This article draws on Export Compliance Guide (B. Flowe, Jr. 1995) and subsequent materials published by the author, including versions of this article published in Coping with U.S. Export Controls (PLI 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010, 2011). I am indebted to major updating and improvements by Dan Fisher-Owens, Partner, Berliner, Corcoran & Rowe, L.L.P., and to many clients and government officials for contributing to my understanding. Readers are recommended to review the excellent overview article, L. Christensen, "Technology and Software Controls under

the Export Administration Regulations," Coping with U.S. Export Controls 2001 666 (PLI 2001). 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 to any specific facts or circumstances.

[2] An export product matrix is a recommended tool for most export compliance programs, which lists export classifications of products and other items a company expects to export, including Export Control Classification Number, destinations to which an item may be exported using the designator No License Required, any applicable License Exceptions and countries for which they may be used. Some companies also include technology or have a separate matrix for technology exports that may require a license (including deemed exports).

[3] EAR Part 772 provides the following relevant definitions:

"Technology". (General Technology Note)-- Specific information necessary for the "development", "production", or "use" of a product. The information takes the form of "technical data" or "technical assistance". Controlled "technology" is defined in the General Technology Note and in the Commerce Control List (Supplement No. 1 to Part 774 of the EAR). N.B.: Technical assistance--May take forms such as instruction, skills training, working knowledge, consulting services. Note: "Technical assistance" may involve transfer of "technical data".

"Technical data".--May take forms such as blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions written or recorded on other media or devices such as disk, tape, read-only memories.

[4] *See* Christensen, *supra*, at 663-67.

[5] Foreign availability of such items has been demonstrated by an Information Security Technical Advisory Committee (ISTAC) report, available from the author on request.

[6] 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 and 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

[7] 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. Supp. No. 3 to EAR Part 740 (2012).

[8] The author can provide on request an excellent article by Ira Rubinstein explaining "crypto with a hole" issues and other details on encryption rules prior to 2004 changes.