EXPORTING TECHNOLOGY AND SOFTWARE, PARTICULARLY ENCRYPTION

Benjamin H. Flowe, Jr.[1]
September 2017

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 laws and government policies concerning technology and software are complex. This discussion summarizes the current rules and special procedures for 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 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 requires export authorization for all destinations from the State Department's Directorate of Defense Trade Controls ("DDTC"). Other aspects of this analysis do not apply to ITAR technology. This analysis also assumes an exporter

---

[1] Partner, Berliner Corcoran & Rowe LLP, Washington DC; JD, Univ. 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 2003-2016). I am indebted to major updating and improvements by Dan Fisher-Owens, Partner, Berliner Corcoran & Rowe LLP, and to many colleagues, 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 recommended for most export compliance programs. It lists export classifications of products and other items a company exports, indicating Export Control Classification Number, destinations authorized under No License Required, and any applicable License Exceptions. Some companies also include technology or have a separate matrix for technology exports (including deemed exports).

[3] EAR Part 772 provides the following relevant definitions: "Technology." Technology means: Information necessary for the "development," "production," "use," operation, installation, maintenance, repair, overhaul, or refurbishing (or other terms specified in ECCNs on the CCL that control "technology") of an item.
N.B.: Controlled "technology" is defined in the General Technology Note and in the Commerce Control List (Supplement no. 1 to Part 774 of the EAR).
Note 1 to definition of Technology: "Technology" may be in any tangible or intangible form, such as written or oral communications, blueprints, drawings, photographs, plans, diagrams, models, formulae, tables, engineering designs and specifications, computer-aided design files, manuals or documentation, electronic media or information revealed through visual inspection;
Note 2 to definition of Technology: The modification of the design of an existing item creates a new item and technology for the modified design is technology for the development or production of the new item.

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). Until recently, exporters could use the symbol "TSPA" on shipping documentation to cover such exports. However, an EAR revision removed the option to use TSPA and advised that NLR should be used instead. 79 *Fed. Reg.* 4613, 4614 & 4619 (Jan. 29, 2014). The revision was characterized as editorial, not substantive, and said the reason for the change was that BIS no longer needed to keep such statistics. The reason the TSPA provision was adopted in the EAR rewrite was because sophisticated software export compliance experts did not want to leave blanks in export product matrices and documentation for publically available software, or anything else. NLR is technically not correct either, because it is used to indicate that an item is subject to the EAR, but no license is required to authorize export. Software exporters may wish to continue using TSPA internally in place of an ECCN. Most exported technology qualifies for publicly available treatment. For instance, most, if not all, hardware 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 therein 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. As confirmed in connection with a major revision to the EAR's definitions, U.S. persons have the First Amendment right to put otherwise EAR-controlled technology in the public domain. 81 *Fed. Reg.* 35586, 35589 (Jun. 3, 2016). 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 ITAR § 120.11. It also does not include basic marketing information on function or purpose or general system descriptions of defense articles. Practitioners have long debated 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. A proposed revision to the ITAR's definition of "public domain" includes posting on the Internet as a mode of publication. See proposed ITAR § 120.11(a)(4), 80 *Fed. Reg.* 31525, 31534 (Jun. 3, 2015). However, as of this writing, DDTC has yet to implement the proposed rule. DDTC also proposed the addition of a new ITAR § 120.11(b), which indicates that technical data or software, whether or not

developed with government funding, is not in the public domain if it has been made available to the public without authorization from either the Directorate of Defense Trade Controls, the Department of Defense's Office of Security Review or relevant U.S. government contracting entity or another government official with public release authority. This proposal triggered an enormous amount of negative comments from the public, as well as pointed questions from Congress about First Amendment compliance and the extent to which such restrictions might inhibit the exercise of Second Amendment rights. At the time of the publication of the rule, and still at the time of this writing, DDTC was involved in a lawsuit brought by a company that had published CAD files for 3D printing of a firearm, and which DDTC had instructed to be removed from the web. The better view on this debate, in this author's opinion, is that information freely available on the Internet is in the public domain, but it remains to be seen how DDTC and the courts will resolve this issue. Thus, companies should be cautious about posting ITAR-controlled technical data on the Internet for the time being unless they are prepared to defend themselves.

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 authorizing statutes for OFAC's Sanctions Regulations and for many years the EAR. 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, Syria and the Crimea region of Ukraine).

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. (Note: A 2006 BIS interpretation of the definition of "use" decontrolled most operations technical data, rendering this license exception less important. See Section 1.1.4 below for further discussion.)

1.1.4. Fourth, to the extent that publicly available treatment or TSU are not available, all technology to be exported must be **classified under the applicable Export Control Classification Number ("ECCN")** on 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 (based on the combination of the 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. See EAR § 740.6. Before using License Exception TSR for such an export, the exporter must obtain a written assurance from the recipient 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.[4]

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) can be used for actual exports, as well as for deemed exports.

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.[5]

When considering whether technology constitutes controlled "use" technology, it is important to consider the BIS interpretation of the term, which was issued 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 determined 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, 30842 (May 31, 2006). Thus, unless the proposed export involves a

[4] The "Foreign National Review" requirement to establish CIV and CTP eligibility was removed. 81 *Fed. Reg.* 64656, 64644 (Sep. 20, 2016).

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

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 "600 Series," added to 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 deliberate, as control over any of these six elements is consistent with the approach to ITAR technical data controls. Both DDTC and BIS have repeatedly stated in the context of the Export Control Reform process that the intent was to shift controls of certain 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 controls on operation or maintenance information.

Another point to keep in mind is that controlled technology remains controlled, even if it happens to be used to produce a non-controlled item. As the General Technology Note 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.) For example, National Security controls apply to certain "development" and "production" technology described in 3E002, even though microprocessors manufactured with such technology are subject to Anti-Terrorism controls only under 3A991.

On the other hand, not all technology relating to a controlled item or listed in a technology ECCN is subject to export controls. Rather, only "required" technology is controlled. 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.[6]

[6] Proposed changes to ITAR definitions in 2015 included addition of a substantially identical definition of "required". See 80 *Fed. Reg.* 31525, 31535 (Jun. 3, 2015) (proposed ITAR § 120.46). Given that many USML entries are not based on specific performance parameters, the proposal had a number of notes providing guidance how to apply "required" and "peculiarly responsible" to USML items. Still, it may be challenging to apply to USML categories not based on objective parameters, such as those that control "military" items. As of this writing, DDTC has not implemented the proposed changes.

For example, for technology to be controlled under 4E001, it must be "peculiarly responsible" for enabling the 4A or 4D item to achieve the performance parameter required for control. If the controlled item is a "digital computer" under 4A003.b, the 4E001 technology must be "peculiarly responsible" for enabling the "digital computer" to exceed 12.5 WT (or other applicable control parameters).

One expert applying the term "required" might conclude that, because all technology to develop or produce controlled computers also is used to develop or produce computers that are not controlled, there is no technology on a production line that is peculiarly responsible for development or production of the controlled computers. Another might conclude 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 analysis is required to determine just what specific technologies are "peculiarly responsible" for achieving relevant control parameters. In the Export Control Reform process, BIS also added three illustrative notes, in an attempt to clarify when technology related to "600 Series" parts and components of ITAR-controlled items is subject to the EAR.

Another aspect of this classification process is which ECCN applies. For example, for computers, the peculiarly responsible technologies may in fact all be Cat. 3 technologies, rather than Cat. 4 technologies. 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 controlled by Cat. 3, not Cat. 4. A computer production line likely does not include such controlled microprocessor development or production technologies.

Similarly, all "required" technologies might be publicly available and thus not controlled.

These are fact questions 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 or 3E002 technology, but there is a limit of 16 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: "Releasing" "technology" 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 § 734.13 and 742.15. For export control purposes, the term "foreign person" 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-cryptographic software currently qualifies for export under NLR or License Exception TSU to all destinations except Embargoed Countries. Note: Many of these provisions rely on the use of License Exceptions. Consult EAR part 740.2 to confirm there are no prohibitions relating to the use of License Exceptions.

1.2.1. All software programs designed for military uses, or directly related to an ITAR-controlled defense article require export licenses to all destinations from the State Department's DDTC. Additionally, ECCN 9D515 and "D" categories the "600 Series" can control software "specially designed" for the "development," "production," operation, maintenance, or installation of defense articles, 600 Series items, and 9X515 items. **Other provisions in this analysis do not address such ITAR, 600 Series, and 9D515 software.** While subject to the ITAR until Dec. 30, 1996, software with commercial encryption functionality is now subject to the EAR, with the level of restriction depending on the type of item and functionality. The use of classified or other military encryption algorithms triggers ITAR control.

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 NLR, as described above in 1.1.1 (including the use of TSPA) for technical data). **Note that certain encryption source code is not eligible for this exclusion unless specified notification requirements are completed. 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 NLR exports as publicly available 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 use of 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 are limited to software related to Chemical/Biological (Column 1) activities, firearms, certain 9X515 satellite-related items, and surreptitious interception of communications.

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. While the OFAC Sudan sanctions were suspended in January 2017, EAR controls on CCL items remain unchanged.

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 is generally 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. However, no software with cryptographic functions can 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 (except 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 Exceptions is applicable, the exporter must work with engineers to classify the software under the applicable ECCN and apply the Country Matrix in EAR Part 738 to determine if NLR or a License Exception applies, or if it must be exported under a License to a particular destination.**

A. Classify the software. Software is covered by Part D of each CCL category:

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 in Part D of Cat. 4 (non-cryptographic), Part D of Cat. 5, Part 1, (cryptographic) or as EAR99. Most non-cryptographic telecommunications software is classified in Part D of Cat. 5, Part 1, or as EAR99. 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, or 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). Before using License Exception TSR, the exporter must 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, subject to compliance with applicable encryption review or self-classification procedures set forth in EAR part 740.17. 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 United States. 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 person (as discussed above in Sec. 1.1.5), so that appropriate decisions can be made on whether disclosure of non-public technical data or source code to that foreign person 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 persons will be eligible to receive most

technical data of the type used by most companies under NLR, License Exception ENC, or License Exception TSR, provided that they sign an appropriate written assurance against reexport of such data or its direct product. Human resources personnel are trained to avoid unlawful discrimination and also are often more sensitive to these "deemed export" compliance requirements, due to the inclusion of certifications related to export compliance in the I-129 forms used to apply for non-immigrant employer sponsored visas, such as H-1 visas. However, many companies still miss foreign persons who are hired while in the United States under a student visa or where another company applied for the visa.

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 § 734.13(b) 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 China 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. Prior to 1994, most exporters believed the release of EAR controlled technical data to foreign persons in the United States would be treated as an "export" only when the person releasing the technology had knowledge that its recipient intended to export it to his or her home country or another country requiring a license. 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 (currently set forth in EAR § 734.13(b). 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 person 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 far fewer enforcement cases than for 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 $289,238 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, and then classify that data. The ECCN will determine whether a license will be required, or whether the access may be provided under NLR or pursuant to License Exceptions such as TSR, TSU, CIV, ENC or others. Again, to facilitate compliance with the deemed export rule, companies should consider developing a technology matrix clearly setting forth applicable licensing requirements.

Whether a deemed export license is required depends on a foreign person's country of nationality and residence, 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 person who are nationals of one of the Embargoed Countries. Licenses will also often be required for nationals of Country Group "D:1", countries which have been identified as a national security risk, including the China, Russia, several former Soviet republics, Iraq, Libya, and Vietnam. Controlled technical data transfers to foreign persons who are 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 person 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 Country Group E countries. Thus, it is advisable to have all foreign person employees sign such an assurance.

Some highly controlled technology and source code is not eligible for TSR, and requires a license prior to "export" to any foreign person 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.

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 § 734.17(a). (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.

Commerce indicated at the end of 1996 that it would start enforcing the deemed export rule, causing a rush to obtain deemed export licenses for foreign person employees. 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 problem, requested the cabinet-level Export Administration Review Board ("EARB")[7] to meet in June 1997, for the first time in seven years, 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.

[7] The EARB is the last level of interagency export control dispute resolution before the President. It is composed of the Secretaries of State, Commerce, Defense, Energy, the Attorney General (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.

Additional standard conditions were released for encryption items. These standard conditions have been revised periodically, and are available as part of the BIS deemed export application guidelines at http://www.bis.doc.gov/index.php/forms-documents/doc_download/709-guidelines-for-foreign-national-license-applications.

In 1997, the standard conditions enabled Commerce to process the backlog and diminished 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, the licenses contain numerous conditions which, in reality, require employers to change the job descriptions of the foreign person employees.

More fundamentally, many U.S. companies believe the deemed export rule impairs U.S. competitiveness, unfairly discriminates against foreign persons, and violates the First Amendment. The U.S. Justice Department reportedly has 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 persons and certain other sensitive personal data, U.S. companies are put in a difficult position, as many think they are prohibited from asking for such information under U.S. anti-discrimination laws, although national security exceptions to employment laws do 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 2000 alleging that enforcement was inadequate. Some have been concerned about the high number of Chinese 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 intra-company 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. After much back-and-forth with industry, BIS published a Proposed Rule to establish License Exception ICT in 2008. 73 *Fed. Reg.* 57554 (Oct. 3, 2008). Industry comments judged the proposed License Exception more burdensome than obtaining individual licenses. Industry groups continue efforts to revise it in some form.

BIS also raised thresholds of technology requiring deemed export licenses related to development and production of computers and microprocessors in November 2004, implementing a "Foreign National Review" submission that was a sort of "lite" license applications. These thresholds were raised from time to time over the next decade or so, and the FNR requirement was removed on Sep. 20, 2016, and replaced with a broader License Exception CTP.

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, rather than risking

enforcement. 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); 70 *Fed. Reg.* 30655 (May 27, 2005). The chief concern to exporters in the OIG's suggested changes was the recommendation that BIS adopt a policy of determining nationality for deemed export purposes based on a foreign person's country of birth, a departure from the current BIS practice of using the most recent country where the foreign national has gained citizenship or the equivalent of permanent residence. 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 residence 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 related 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 over 300 comments, the most up to that time on a proposed or interim EAR amendment. 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 EAR's "fundamental research" definition and the proposal that deemed export licenses be required for foreign persons based on merely having access to export controlled equipment. Industry took primary aim at the "country of birth" proposal. We assisted several clients in preparing comments and also contributed to comments submitted by the American Bar Association. All comments are available at https://efoia.bis.doc.gov/index.php/component/docman/?task=doc_download&gid=724&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 the advance notice of proposed rulemaking. 71 *Fed. Reg.* 30840 (May 31, 2006). Many were surprised that BIS refrained from making a few of the less controversial modifications, 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 recommendations for deemed export reform. The DEAC issued its report in December of 2007, making several high-level recommendations, 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 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 technology ECCNs 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 https://efoia.bis.doc.gov/index.php/component/docman/?task=doc_download&gid=734&Itemid=526. 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. Integration of lower level military items into the EAR with Export Control Reform seems to have significantly reduced the likelihood that the Administration will support material relaxation of deemed export controls in the near future, even though the vast majority of license applications are approved, and one of the goals of ECR was to reduce "routine" license requirements.

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 persons, 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 persons who are sponsored in high-tech companies for non-immigrant 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. Employers should not see the I-129 process as a completely effective means of checking for deemed export issues. Employers frequently hire foreign persons who are already in the country on an employment visa issued to another employer, or that flows from a foreign person's student visa.

Violations of the deemed export rule can, of course, also lead to EAR or ITAR fines and penalties, including denial of export privileges, and debarment, separate and apart from any immigration violations that may occur.

BIS also reported in its 2009-2016 annual reports that it has made hundreds of outreach visits per year (743 in FY 2016) focusing on deemed export compliance, and followed dozens of leads and cases involving alleged deemed export violations. Export Enforcement officials have stated time and again that the deemed export rule is a BIS enforcement priority.

In the first major deemed export enforcement, 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 was the first instance in which civil or criminal charges were brought 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 involved 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 really needed to support that count.

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, a $275,000 administrative penalty and a twenty-year denial of export privileges (although Suntek's administrative penalty was waived). Kuan also agreed to pay an administrative penalty of $187,000 and to a twenty year denial of export privileges. (There is also a risk of deportation for foreign persons recipients of 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). Chinese national employees were involved in three of the four cases; the Pratt & Whitney case also involved deemed exports to EU nationals.

There was 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 deemed export violations only.

There were several other cases in the same time frame 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, with 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.

A 2014 case against Intevac, Inc. involved four charges related to deemed exports to a single Russian employee, as well one charge involving an unrelated export of technology to China. Intevac agreed to a penalty of $115,000. BIS charged multiple violations because Intevac, having identified the need to obtain a deemed export license for the employee, and having already applied for it, did not restrict the Russian national's access to the controlled technology.

Perhaps the take-home point in these cases is summed up by comments by Julie Salcido, then Special Agent in Charge of the OEE San Jose Field Office at a 2013 conference on technology controls. Special Agent Salcido remarked that her agents pursue deemed export cases since they are easy cases to make, because OEE needs only to establish the nationality of a foreign person employee, and that the foreign person had access to controlled technology. Defending such a case can also involve the formidable task of proving that a foreign person 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 within 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 persons 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 persons sign Non-Disclosure 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 foreign persons working legitimately in U.S. companies.

Deemed export license applications require firms to provide detailed information on the foreign person'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 person will have access. Applications must indicate whether the foreign person 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 authorizing 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 person 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 deemed export license applications were averaging about 36 calendar days to process, but more recent annual reports have not broken out deemed export license processing time as a separate statistic. 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 remain some of the most complex and difficult in the EAR, despite much liberalization since 1996. That is in part because, until Sep. 2016, Note 1 to CCL Cat. 5, Part 2 (Information Security), stated a "see-through" rule:

> 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.[8]

Decontrols in 2010 and 2016 reduced the circumstances where this "see-through" rule applies, but exporters still need to consider encryption in their classification process to one degree or another.

The complexity of the U.S. encryption regime is also a vestige of numerous incremental changes to controls on cryptographic products 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 EAR a "Virtual ITAR" within the EAR. Nearly annual policy changes have included the proposed "Clipper Chip," a failed policy favoring Key Escrow techniques, a failed policy to allow exports of 56-bit encryption items based on promises to develop Key Recovery products, easing 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 and other close allies, liberalization of "Mass Market" products, and more carve-outs and special considerations that created quite a maze of provisions.

This section summarizes the most recent substantial revisions of 2010, 2016 and 2017, explains the structure of the current EAR encryption controls, and then walks you through a way to analyze products containing encryption functions from the least restrictive through the most restrictive controls.

3.1 ENCRYPTION REVIEW AND REPORTING STREAMLINING AND ANCILLARY "NOTE 4" IMPLEMENTATION. A lengthy interim final rule published on June 25, 2010, implemented the Obama Administration's March 11, 2010, promise to replace

[8] In Sep. 20, 2016, BIS moved this note to the General Technology and Software Notes in Supp. No. 2 to EAR 774 and revised it to read as follows: 3. *General "Information Security" Note.* "Information security" items or functions should be considered against the provisions in Category 5-Part 2, even if they are components, "software" or functions of other items.

(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 reporting by registrants of new or changed encryption products.

The rule also implemented Note 4 to CCL Cat. 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. This Note had been added to the Wassenaar Arrangement Dual-Use list at the instigation of the United States in December of 2009. (As will be discussed later, the concept of Note 4 was incorporated into a revised item description of ECCN 5A002 in 2017, implementing changes agreed to in the 2016 Wassenaar plenary meetings.)

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 was the first step in truly streamlining and clarifying the cumbersome and overly complex encryption controls. The 2010 restructuring did remove controls on many items, and substituted an arguably more self-driven process.

There have been additional reforms since 2010, and 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. 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 to Note 3 were implemented by BIS in mid-2013. 78 *Fed. Reg.* 37372 (Jun. 20, 2013). Software components for mass market items received similar treatment at the December 2013 Wassenaar Plenary meeting, and BIS added provisions to clarify that executable software for hardware excluded from 5A002 by the Mass Market Cryptography Note are also accorded mass market treatment, among other changes. 79 *Fed. Reg.* 45287 (Aug. 4, 2014).

Cat. 5, Part 2, was restructured again in the Wassenaar 2015 plenary meetings. ECCN 5A002 was reorganized, and certain non-cryptographic items were moved to new ECCNs 5A003 and 5A004. In implementing these changes on Sep. 20, 2016, BIS also took the opportunity to streamline certain aspects of the EAR to consolidate them into EAR § 740.17, and also applying decontrols to certain low-strength encryption and limited encryption items, which in some cases drops them to EAR99 classification. Adding to the January 2011 rule, publicly available encryption source code can be released from EAR jurisdiction upon filing a notice of its internet location. Certain other aspects of the registration and reporting requirements were further simplified, as will be described further below.

Additionally, in August 15, 2017, BIS implemented changes to the structure of ECCN 5A002 agreed to in the Wassenaar 2016 plenary, which essentially integrate the Note 4 "Ancillary" concept into the positive description of what items are controlled under ECCN 5A002.a, although the wording was changed slightly.

3.1.1. <u>Overview of Review and Reporting Streamlining for Most ENC-U and Mass Market Products</u>. Prior to 2010, most 5D002 and 5D992 encryption items were subject to a mandatory 30-day encryption classification review or notification process, imposing varying levels of delay before companies could release their products. The 2010 changes moved a long way toward permitting exporters to self-classify most mass market and ENC-Unrestricted cryptographic items, which is the norm for non-crypto products, but certain hurdles remain. From 2010 to 2016, use of the "self-classification" provisions was subject to a requirement to obtain an Encryption Registration Number ("ERN") before exporting and to report the items self-classified at the end of the year. The September 2016 rule eliminated the ERN requirement, and permits exporters to satisfy the reporting requirement by either obtaining a formal classification ruling from BIS or filing a post-export annual self-classification report.

The good news is that, for most products, exporters do not need to hold up new product distribution awaiting filing and review of applicable encryption classifications, less information needs to be reported in the annual reports, and there should be less need for second guessing by BIS/NSA of whether items qualify as 5X992 Mass Market vs. 5X002 ENC, because there are fewer distinctions in the level of controls.

The 2010 and 2016 rules added new complexities in that License Exception ENC (EAR § 740.17) now comes in more flavors:[9]

> (a)(1)(i) for exports without BIS prior review to private sector end-users headquartered in EAR Part 740, Supp. 3, countries for internal development end-use, without review
>
> (a)(1)(ii)(added by the Sep. 20, 2016 rule) to allow any type of end-use, provided that the item is subject to the EAR after produced, all parties to the transaction are subsidiaries of the same parent company headquartered in a Supp. 3 country, and the characteristics or capabilities of the item are not enhanced, unless otherwise authorized.
>
> (a)(2) for exports to "U.S. subsidiaries" for any internal end-use without BIS prior review (no change)
>
> (a)(3) (formerly paragraph (b)(4) prior to Sep. 20, 2016) for 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).
>
> (b)(1) for 5X002 and 5X992 exports of any items <u>not</u> covered by (b)(2) <u>or</u> (b)(3). Such items can be exported immediately, subject to either obtaining a formal BIS classification, or filing of an end of year reporting of self-classification of all such products in spreadsheet format with some details about the manufacturer and exporter, but not with the level of detail required by Supp. 6 to Part 740 (unless requested). The Sep. 2016 rule moved the self-classification and reporting provisions for 5X992 mass market items to this section to minimize the duplicative aspects of former 742.15(b)(1).
>
> (b)(2) for items such as network infrastructure, based on technical parameters, non-published source code, and others as specified, but now also including items with penetrating capabilities

[9] The Jun. 2010 rule re-shuffled the paragraphs of EAR § 740.17 and § 742.15; the Sep. 2016 rule further re-arranged the paragraphs of EAR § 740.17, and consolidated mass market-related provisions formerly in EAR § 742.15 into EAR § 740.17. So, for rulings prior to Jun. 2010, and in some cases between Jun. 2010 and Sep. 2016, may require translation between old and new paragraph numbers.

that are capable of attacking, denying, disrupting, or otherwise impairing the use of cyber infrastructure or networks (existing classifications are grandfathered), public safety radios, certain ultra-wideband and spread spectrum items, as well as cryptanalytic and open cryptographic interface items; items in this category require the same full encryption classification application and approval, as well as reports of actual exports every six months. Items in this category are not eligible for mass market treatment.

(b)(3) 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. Items in sub-paragraph (iii) require semi-annual shipment reporting and are ineligible for mass market treatment; only items (i), (ii) and (iv) are eligible for mass market treatment, but eligibility must be confirmed by BIS:

(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 non-published 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).

The June 25, 2010 rule permitted technology to be exported under ENC-R, after full classification review by BIS, to non-Government end-users in destinations other than Country Groups D:1 or E, or to the Crimea Region of Ukraine, 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 made changes in 2011 and 2016 that released open object code and open source code, respectively, from EAR jurisdiction after an e-mail notification to BIS and NSA.

Exporters can still seek formal classification rulings for any product, just as with other ECCNs. Exporters just are no longer required to do so for EAR § 740.17(b)(1) items. Such optional classification requests can be reviewed by BIS without review by other agencies. As of 2010, exporters also no longer need to make a separate submission for required classifications to the ENC Request Coordinator (NSA); BIS forwards submissions to NSA when required, as it does for license review by other agencies.

3.1.2. "Ancillary" and Wassenaar Note 4 Implementation and Further 2016 Decontrols. In October 2008, BIS allowed 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 United States persuaded Wassenaar members to decontrol such products altogether via Note 4 to CCL Cat. 5, Part 2, adopted at the Wassenaar plenary meeting in December 2009. Exporters can self-determine eligibility for Note 4, which removes from Cat. 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, such items are removed from CCL Cat. 5, Part 2, altogether. 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 Jun. 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 had been discussed in BIS presentations to industry.[10] We think these examples should be included in the EAR itself, either in a new commodity interpretation (EAR Part 770) or in Supp. No. 3 to EAR Part 774, Statement of Understanding. BIS has included them in Frequently Asked Questions on its website. The term "ancillary" has been dropped, but is sometimes used informally. Items formerly self-classified or classified by BIS as "ancillary" following the Oct. 3, 2008, rule were grandfathered into Note 4 eligibility and no longer classified under Cat. 5, Part 2. Of course, exporters can seek a formal BIS classification to confirm exclusion, but are not required to do so.

In the Sep. 20, 2016, rule, BIS further decontrolled to EAR99 items that had formerly been placed in ECCN 5A992.a and b or 5D992.a and b. Such items are those that do not meet the Note 4 criteria, but use only low-strength encryption below the thresholds listed in ECCN 5A002, or have only limited cryptographic functionality, such as authentication or password-only encryption, as well as various listed categories of limited cryptographic functionality (See Section 3.3.3 below).

On Aug. 15, 2017, BIS implemented changes to the structure of 5A002 intended to eliminate the "catch and release" of Note 4, and instead integrate the exclusion of "ancillary" items into the text of the relevant ECCNs. 82 *Fed. Reg.* 38764 (Aug. 15, 2017). Now, 5A002.a.1 applies only to those items whose primary function is information security, digital communications and networking equipment and systems, computers, items with information storage or processing as a primary function, and – relying on the ITAR-style "see-through" rule – other items that don't have any of these primary

[10] 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

functions, but incorporate a 5A002 or 5D002 item to support a non-primary function. While BIS indicated in the preamble to the Federal Register notice that there was no intent to change the scope of Note 4, unfortunately, none of the new terms are defined, and none of the prior guidance concerning the types of excluded items was included in a commodity interpretation or otherwise put into the regulations. We think BIS should do so in the future, to ensure that all exporters get the full benefit of decontrols, particularly since it took BIS almost nine months to update its web guidance after the September 2016 changes.

3.1.3. Benefits and Drawbacks of the 2010 and 2016 Streamlining Rules. The 2010 restructuring was the first major change to encryption regulations since 2002, and most of the 2016 changes were focused on streamlining the provisions, without significant relaxations of controls. For most ENC-U and mass market items, you can simply self-classify products throughout the year, and submit a self-classification report at the end of the year. Removal of requirements for six-month reporting of shipments for most ENC-U sales and streamlining of product submissions for most mass market and ENC-U products were welcome improvements. The ability to get technology approved under License Exception ENC for export beyond just "U.S. subsidiaries", and including broader authority for FTC headquartered companies was also a welcome improvement. One welcome facet of the 2016 rule was an expansion of the scope of permissible destinations for certain ENC-Restricted items.

Unfortunately, despite the 2010 and 2016 changes, the encryption provisions remain the most confusing part of the EAR for most exporters and regulators. The Orwellian split making some products "more mass market than others" is particularly unfortunate, given that most Wassenaar countries permit self-classification of any mass market product. 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.

The 2016 changes made the rules slightly more manageable for exporters, eliminated some of the need to skip to and from several parts of the regulations, decontrolled certain items that did not have any strategic or security importance, and made the reporting requirements less confusing. Some performance parameters on ENC-R items were raised, but overall the rules remained fundamentally the same.

While the opportunity to self-classify is attractive, one must still be accurate when self-classifying under a strict liability regime. So, be sure to check facts carefully, document the classification rationale, and use these revised regulations to improve compliance. Exporters can still obtain formal CCATS classifications instead of self-classifying. 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.

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. While the 2010 and 2016 changes were welcome, the encryption provisions of the EAR still remain the most complex and least penetrable. Industry is still pressing to eliminate additional restrictions, such as removing the tight controls on open cryptographic interfaces for mass market and ENC-U items, which do not apply to open source products and are not maintained by other Wassenaar countries; eliminating the remaining vestiges of the ITAR "see through" rule from the EAR; consolidating or eliminating reporting

requirements; dropping review requirements for all mass market and ENC-U products; and increasing ENC-R thresholds based on foreign availability[11].

3.2. STRUCTURE OF ENCRYPTION CONTROLS. EAR encryption controls are principally in:

Part 774, Supp. 1, Commerce Control List ("CCL"). Cat. 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 Exception ENC (or other situational License Exceptions, 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 the description in ECCN 5A002.a, and in Notes at the beginning of the category and in a "related controls" section.

Items decontrolled based on not meeting the ECCN category description in 5A002.a, or excluded by the Medical Note, Related Controls Notes or Category Exclusion Notes, drop out of Cat. 5, Part 2, completely. Items that are decontrolled under the Note 3 mass market provision move to ECCNs 5A992.c, and 5D992.c, and 5E992.b ("use" technology), which allow exports under NLR to all countries except Embargoed Countries.

Part 742.15 states encryption licensing requirements and policy and the requirements for making e-mail notifications of the location of publicly available source code (which were relocated to 742.15(b) from License Exception TSU, EAR § 740.13(e), in 2016). Key instructions are also found in two Supplements to Part 742: Supp. 6 for information required for mandatory classification requests and Supp. 8 for self-classification reports.

Part 740.17, License Exception ENC, the primary License Exception (discussed below) for exporting 5X002 items, and as of 2016, mass market 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) submits by February 1 of the following year an annual report describing the items classified, or obtains an optional classification ruling. For exports of more sensitive 5X002 items, submission of a classification request and a 30-day wait for a response from BIS is required, as well as semi-annual reporting of actual exports.

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.

[11] Foreign availability has been demonstrated by an Information Security Technical Advisory Committee (ISTAC) report, available from the author. RPTAC and industry group recommendations for further improvements are also available on request.

Part 734.17 has a special definition of "export" for 5D002 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 Encryption Item Is a Medical End-Item. Interpretation13, EAR § 770.2(m),[12] provides that "commodities and software specially designed for medical end-use that incorporate an item in Category 5 - Part 2 are not controlled 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 ECCN or EAR99. Note that the encryption itself does not need to be restricted to a medical function, but rather the functionality of the end-item determines eligibility. You 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 Wassenaar "medical note" in Supp. No. 3 to EAR § 774.

3.3.2. Determine Whether Encryption Item Is Excluded by the Text of 5A002 Based on Primary Function (Equivalent to Exclusion under Former Note 4 to CCL Category 5, Part 2. Items that use encryption, but whose primary function is not information security, digital communications or networking; or computers and other items with a primary function of information storage or processing, are excluded from control under Cat. 5, Part 2. The August 2017 changes to the EAR implemented revisions to the Wassenaar Arrangement control list that were agreed to in December 2016, which were intended to integrate former Note 4 to Cat. 5, Part 2, into the ECCN description for 5A002. In its implementing regulation, BIS indicated that it did not intend to change the scope of items controlled, but the changes to the structure and language could raise some questions.

In particular, exporters have been challenged since the implementation of Note 4 to understand whether their items are supposed to be within the scope of 5A002, and BIS did provide some examples. The Jun. 25, 2010, Federal Register notice implementing Note 4 contained a non-exhaustive list of examples of types of products that qualified for Note 4 in the preamble; (see Section 3.1.2 above). 75 *Fed. Reg.* 36482, 36487-88. Exclusion from the scope of 5A002 is driven by the product's primary functionality, not by how or what encryption is used. Exporters can self-determine exclusion from the scope of 5X002 on the basis of primary functionality, or have the option to 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 Oct. 3, 2008 and Jun. 25, 2010 were grandfathered as eligible for Note 4, and classification rulings confirming Note 4 eligibility from 2010-2017 are still reliable.

[12] This provision was formerly N.B. to Note 1 of Cat. 5, Part 2, and was moved to EAR § 770.2(m) by the Sep. 20, 2016 rule.

Items that use cryptography solely for intellectual property, digital rights management, and/or copy protection/license management are also excluded. Such items were formerly decontrolled to 5D992 under 5A002 Related Controls notes before 2010, but were excluded from Cat. 5, Part 2, when Note 4 was implemented. This exclusion was not very clear in the regulations themselves, but it is clearly stated in the preamble to the Jun. 25, 2010 Federal Register. 75 *Fed. Reg.* 36482, 36487. The exclusion was moved to "Technical Note 1" to clarify that such items are not subject to control under 5X002. 82 *Fed. Reg.* 38764, 38800 (Aug. 15, 2017).

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

3.3.3. Determine Whether Encryption Is Excluded from Category 5, Part 2 under the Item Description of 5A002.a and Following Notes (Without Notification or Review). Encryption items also can be excluded from Cat. 5, Part 2, controls 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.

Items specifically excluded from control under 5A002, by virtue of the category description, or that have limited cryptographic functionality, have long been eligible for self-classification under 5X992, but were removed from Cat. 5, Part 2, by the Sep. 20, 2016, rule. Eligible items were consolidated from the Related Controls note and other parts of EAR § 740.17 and § 742.15 and are now listed in Technical Note 1" following ECCN 5A002.a. Examples are items where cryptographic functionality is limited to digital signature, authentication, fixed coding or compression techniques.

"Note 2" to 5A002.a excludes other items based on their specific function, including personalized smart cards, cryptography limited to money or banking functions, and telephone handsets not capable of end-to-end encryption. This exclusion is also where "short-range wireless" and "personal area network" items are listed (they were formerly in EAR § 740.17(b)(4) and § 742.15(b)(4)). An exclusion for computers, switches, routers, and similar equipment, where cryptographic functionality is limited to "operations, administration, and maintenance," is now located in 5A002.a Note 2, paragraphs (h) and (i).

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

Note: It is possible for decontrolled items to drop all the way to EAR99 classification. Even if a product is not subject to EI controls, an exporter must ensure it is not subject to control under another ECCN. For example, short-range wireless items might be exempt from encryption controls, but could be controlled by ECCN 5A991. In practice, BIS applies the most restrictive ECCN applicable to a product, which is why encryption controls are a principal concern, but they are not the only export controls that may apply.

3.3.4. Foreign Products Incorporating U.S. Encryption. Foreign products can qualify for reexport under ENC without prior review, even if they incorporate U.S.-origin encryption components, provided that the U.S.-origin items are qualified for export. This includes foreign-made items that call on U.S.-origin cryptographic interfaces or libraries. However, foreign items are subject to any applicable encryption registration or prior review requirements if the foreign item is 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 U.S. customers can export them easily. Classification requests for foreign items in this category should make it clear that they are foreign origin, and not subject to the EAR unless present in the United States.

3.3.5. Mass Market Items. Mass Market items not mentioned previously require either the exporter or manufacturer to self-classify and file an annual report, obtain an optional classification, or for mass market components described in EAR § 740.17(b)(3), to file a mandatory 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 reports, as follows.

Cat. 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. A simple price inquiry is not considered to be a consultation.

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.

Former EAR § 742.15(b)(6) was eliminated in the September 2016 rule, but provided an illustrative, but not comprehensive, list 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.

Items listed in EAR § 740.17(b)(3) are not eligible for 5X992 Mass Market classification until 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 mass market cryptographic enabling items. Upon filing of the encryption review request described below, other mass market items are eligible for export as 5X002 ENC-Unrestricted items to the Favorable Treatment Countries ("FTCs")[13] and subsidiaries of companies headquartered in FTCs.

All other Mass Market items fall into EAR § 740.17(b)(1), and are eligible for self-classification as 5D992 Mass Market, subject to the annual reporting requirement. Note that an exporter who is exporting a vendor-supplied Mass Market (b)(1) item may rely on issued report made by the manufacturer that covers the manufacturer's item.

However, there is an important exclusion. Items described in License Exception ENC, EAR § 740.17(b)(2) – known informally as "ENC-Restricted" 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, if they are not sold directly to the general public, even if sold in large quantities for use in mass market items,. Now, existing hardware components (and related firmware, but not application software) that were formerly ineligible can qualify for mass market, subject to a prior review requirement. The June 20, 2013 rule added a new paragraph b to Note 3, as amended in August 2014, making the following items eligible for mass market treatment:

> ***b***. *Hardware components or 'executable software' 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 or 'executable software';*
>
> ***2***. *The component or 'executable software' 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 or "executable software" 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 or 'executable software' and relevant end-items are accessible and will be provided to the authority upon request, in order to ascertain compliance with conditions described above.*
>
> Technical Note: For the purpose of the Cryptography Note, 'executable software' means "software" in executable form, from an existing hardware component excluded from 5A002 by the Cryptography Note.

[13] FTC Countries: Austria, Australia, Belgium, Bulgaria, Canada, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, and the United Kingdom. Supp. No. 3 to EAR Part 740 (2016) (the only change since 2010 was adding Croatia in 2016).

Note: 'Executable software' does not include complete binary images of the "software" running on an end-item.

Such items fall into EAR § 740.17(b)(3), which covers chipsets and similar components, which still require a prior BIS classification review.

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. 5X002 Items - Exports to U.S. and FTC Subsidiaries. 5X002 items can be exported under ENC without filing annual self-classification reports 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). The 2016 rule expanded eligibility to authorize exports between and among subsidiaries of Supp. 3 headquartered private sector end-users for items for internal use, provided no modifications are made to the items. 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. Publicly Available Source and Object Code. Open source code and free compiled object code derived from open source are now exempt from EAR, as publicly available items, provided that the notification set forth in EAR § 742.15(b) has been made.

Prior to 2011, the United States asserted jurisdiction over U.S.-origin open source code and object code, subject to export under License Exception TSU, which required notifications to BIS and NSA and prohibited exports to embargoed countries. On January 7, 2011, BIS removed 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 has been published and a notification submitted to BIS and NSA. 76 *Fed. Reg.* 1059 (Jan. 7, 2011).

Publicly available software, other than encryption software, was already outside the scope of the EAR, but certain publicly available encryption software remained subject to the EAR as part of the compromise struck in 1996 to transfer control of commercial encryption items from the ITAR to EAR. As confirmed by BIS in the context of 2016 changes to certain EAR definitions,[14] there are no regulatory prohibitions 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). Once it is "publicly available", and available for download without restriction, BIS finally decided to recognize the obvious – in part - and remove object code from the jurisdiction of the EAR in 2011, and then expanded it to exclude open source code in 2016, subject to the notification requirement.

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 to Iran, Sudan, and Cuba. These changes were intended to legalize exports of such software in response to the use

[14] See 81 *Fed. Reg.* 35586, 35589 (Jun. 3, 2016).

of free 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 § 740.17(b)(3), or
- Self-classified as mass market eligible pursuant to EAR § 740.17(b)(1); or
- Qualified as the product of publicly available source code, qualified in accordance with the procedures in EAR § 742.15(b).

Note that, to use the second option of self-classifying encryption software as mass market, you must subsequently submit an annual self-classification report listing the item.

Proprietary software incorporating or calling on publicly available software remains subject to the EAR because the calling 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 be used only with proprietary products. The uncertainty arises because such items are useful only for the product being patched or updated. However, BIS personnel have informally cited such free updates or drivers as examples of "freeware" that qualifies as publicly available, and it appears that most patch providers do not screen their downloads in practice.

This rule is a welcome, long awaited development that makes the EAR more consistent with OFAC's 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."

The September 20, 2016, rule expanded the scope of the publicly available exemption to cover source code, provided the URL location of the source code or object code has been e-mailed to BIS and NSA. While having no notification requirement would ultimately "normalize" open source encryption, a mere e-mail notification is a minimal impediment to the free distribution of such software.

3.3.8. 5X002 Items Not Listed in EAR § 740.17(b)(2) or (b)(3) Qualify for 740.17(b)(1). Non-Mass Market, 5X002 items other than those listed in EAR § 740.17(b)(2) or (b)(3) can be self-classified and determined to be eligible for ENC-Unrestricted if the exporter or manufacturer complies with the annual self-classified product report requirement described above and below. EAR § 740.17(b)(1). Optionally, if the exporter obtains a classification ruling from BIS, there is no reporting requirement. (It should be noted, however, that changes to cryptographic functionality trigger the need for a new classification ruling or a self-classification report.)

3.3.9. 5X002 Items - 740.17(b)(2) and (b)(3) Items. Items listed in EAR § 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 and technology listed in EAR § 740.17(b)(2)(iv)(B), are subject to distribution restrictions, even for government end-users within the FTC. Most other 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 some

ENC-Restricted items – in particular open cryptographic interface items and technology for "non-standard" cryptography – require a license to be exported to non-government end-users (as well as government end-users) outside the FTC destinations who are not headquartered in a FTC country.

Beginning in September 2016, "network infrastructure" items identified in EAR § 740.17(b)(2)(a)(i)(A) are authorized to be shipped to "less sensitive government end-users" under License Exception ENC. 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. The September 2016 rule also introduced definitions of "less sensitive government end-users" and "more sensitive government end-users" into the regulations, relevant to the aforementioned relaxation for network infrastructure items, as well as to processing of Encryption Licensing Arrangements (ELAs), discussed below.

ENC-Unrestricted items under EAR § 740.17(b)(3) may be exported to all end-users in all but Country Group E and the Crimea Region of Ukraine.

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

- Prior Review Requirements Not Met for EAR § 740.17(b)(2) and 740.17(b)(3) items
- Cryptanalytic Items to Government End-users
- Open Cryptographic Interface to Non-FTC & Non-FTC Subs
- Exports to Country Group E (Cuba, Iran, North Korea, Sudan, Syria), and the Crimea Region of Ukraine
- Source Code or Technology to Country Group E Nationals or residents of the Crimea Region of Ukraine

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

3.3.11.1. Annual "Self-Classification" Report. The other prerequisite to self-classification and eligibility for ENC or Mass Market under EAR § 740.17(b)(1) is submission of an annual report advising BIS and NSA what items have been self-classified during the prior year. Reports are due on February 1st for the previous year. The information required is found in Supp. 8 to Part 742, and is much more general than the Supp. 6 information required for a mandatory classification request. The reports must be submitted electronically in comma-separated value (.csv) format. A report must be filed each year, even if there is no change to cryptographic functions.

Prior to the Sep. 20, 2016, changes, BIS advised that EAR § 740.17(b)(1) (and former EAR § 742.15(b)(1)) items submitted to BIS for voluntary formal classifications must be included in the report. The 2016 changes eliminated this requirement, and no longer require a self-classification report if an exporter has obtained a BIS classification ruling.

3.3.11.2 Clarification of Information Required for Encryption Classifications. While EAR § 748.3(d) still indicates the information in Supp. 6 to Part 742 is required for encryption classifications, EAR § 740.17(d) clarifies that Supp. 6 information must be submitted only for mandatory classification requests for EAR § 740.17(b)(2) and 740.17(b)(3) items. Optional classification requests require only information sufficient to allow BIS to confirm the item is not classified under EAR § 740.17(b)(2) or 740.17(b)(3). The SNAP-R form has a box that says "Check here if you are submitting information about encryption required by 740.17 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 5X002 EAR § 740.17(b)(2) and 740.17(b)(3) items, the second for 5X992 EAR § 740.17(b)(3) items seeking mass market confirmation, and the third option for any other encryption items submitted for review, such as optional classifications for 5X002 or 5X992 EAR § 740.17(b)(1) items or seeking confirmation of exclusion based on non-primary function.

3.3.11.3. 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 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. Exporters can check the STELA system to ensure their 30-day clock is still running, but STELA does not have a status history feature, and you will not receive a notice if your application is put on HWA, unless BIS simultaneously issues a request for information, so it is prudent to check on pending classification requests routinely during the 30-day period, especially if you are cutting it close to an intended release date.

Applicants do not need to request *de minimis* eligibility. 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 Some 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 EAR § 740.17(b)(2) ENC-Restricted items and EAR § 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 must report only their exports to those distributors, and need not collect information on further sales in the distribution chain. However, if the exporter collects end-user name and address information for distributor sales 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 exporters will not be held to the accuracy of the many "Bill Gates" or "Darth Vader" registrations that they report). 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.

To the extent still captured by EAR § 740.17(b)(2) or EAR § 740.17(b)(3)(iii), EAR § 740.17(e) retains reporting exemptions for items with no more than 64-bit symmetric encryption; items exported by free and anonymous download; items from or to a U.S. bank, financial institution or its subsidiaries, affiliates, customers or contractors for banking or financial operations; short-range wireless items, and foreign-manufactured items incorporating U.S.-origin encryption components (except those exported from the United States).

The EAR had seemed to invite exporters to request further reporting relief in specific applications if they could provide adequate justification. To our knowledge, BIS has granted such relief only via interpretations of the existing regulatory exclusions, rather than by 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 obtained such exemptions while those rules were in effect.

However, the June 25, 2010, rule eliminated the provision for asking for and obtaining a product specific reporting exemption, apparently because the rule diminished the scope of the reporting requirements so much. Still, BIS officials have informally said they will continue to entertain 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 EAR § 740.17(b)(2) and EAR § 740.17(b)(3) authorize export 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 EAR § 740.17(b)(2) ENC-Restricted and EAR § 740.13(b)(3) items), but then may immediately make such exports. Again, exports for internal use, and for development of new products by private sector companies headquartered in the FTC and their subsidiaries do not require registration of a review request pursuant to EAR § 740.17(a)(1)(i)-(ii).

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 ineligible government end-users unless authorized under the EAR, and that their distributors and resellers understand that they may not export, reexport, or even transfer within non-U.S. countries to government end-users any ENC-Restricted products unless authorized under the EAR. We recommend obtaining certifications from distributors and end-users with respect to such exports.

EAR § 734.17(c) provides clear guidelines on requirements for posting ENC-Restricted encryption products on the Internet, with warnings about the "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) provides that proprietary encryption source code that is not publicly available pursuant to EAR § 742.15(b) is treated 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 EAR § 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.[15] In contrast, open cryptographic interfaces in open source products are excluded from EAR jurisdiction after the required EAR § 742.15(b) 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, and subsequent versions of the Microsoft operating

[15] 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.

system with OCIs, 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(a)(3). 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, Supp. 6 information as sufficient to. These were informal interpretations, though provided in public meetings. So, for example, if an item called on Windows through the Microsoft Crypto API, and had no other controlled crypto functions, it would take on Windows'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 and NSA have been placing restrictive conditions on the export and use of WAPI and possibly other nonstandard cryptography since the June 25, 2010 rule.

BIS introduced additional definitions in the September 2016 rule, distinguishing between "less sensitive government end-users" and "more sensitive government end-users." BIS had adopted a practice of granting global or regional ELAs for less sensitive government end-users, and requiring country-by-country licensing for more sensitive ones. This distinction has now been incorporated in the licensing policy for ELAs set forth in EAR § 742.15(a)(2), and as mentioned above in Section 3.3.9, certain network infrastructure items can be exported to less sensitive government end-users under License Exception ENC-Restricted. The lists are extensive, and based on our experience parsing them when they were informally provided by BIS, there are inevitably gray areas.

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). EAR § 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. (Note that EAR § 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 long-standing "dormant crypto rule" used to be provided only obliquely in ENC and mass market

encryption regulations. However, BIS amended the EAR on May 20, 2011, to state the "dormant crypto rule" more explicitly. 76 *Fed. Reg.* 29610 (May 20, 2011). This provision was modified slightly and relocated to decontrol note (g)[16] in the September 20, 2016 rule. However, that note was removed by the August 15, 2017, rule, and replaces with text in the introductory paragraph of 5A002.a that indicates only items where the cryptographic functionality is "useable" or has been "activated" is controlled.

This change to the EAR implemented a 2010 revision to the Wassenaar List. Between 2011 and 2016, software or hardware with dormant crypto as classified under ECCN 5D992 (software) or 5A992 (hardware), but the September 2016 rule removed such items from Cat. 5, Part 2.

EAR § 772.1 defines "cryptographic activation" as the following:

> Any technique that activates or enables cryptographic capability, via a secure mechanism that is implemented by the manufacturer of the item and is uniquely bound to the item or customer for which the cryptographic capability is being activated or enabled (*e.g.*, a serial number-based license key or an authentication instrument such as a digitally signed certificate).
>
> TECHNICAL NOTE TO DEFINITION OF ''CRYPTOGRAPHIC ACTIVATION'':
> ''Cryptographic activation'' techniques and mechanisms may be implemented as hardware, ''software'' or ''technology''.

An exporter using the dormant crypto rule must restrict export of the cryptographic activating technique (*e.g.*, key, certificate, etc.) as if it were the crypto enabled hardware/software. Items that enable 5A002.a cryptographic functionality are controlled under 5A002.b (hardware), 5D002.d (software), and 5E002.b (technology), although we believe normal encryption classification rules would apply (*e.g.*, items that activate crypto mass market would be controlled as 5X992, and those that activate exempt items would not be controlled in Cat. 5 Part 2).

Further, under the June 25, 2010, revision, items that enable cryptographic functionality are not self-classifiable under the provisions of EAR § 740.17(b)(1) – even if the activated item otherwise qualifies for self-classification as ENC or mass market eligibility. Exporters using the dormant crypto rule should make sure they can control the cryptographic activating techniques (*e.g.*, keys) effectively, as that is often harder to do. If you treat the original export as encryption controlled, then the export of the cryptographic activating technique (*e.g.*, key) is normally treated as only an export of uncontrolled data, though this is not specified directly in the regulations, only by implication.

3.5. UPGRADES TO KEY LENGTHS AND SUBSEQUENT BUNDLING. EAR Part 740.17 permits reporting for upgrades to encryption key lengths for 5X002 items (but not mass market items), without having to submit a new classification request. *See* EAR § 740.17(e)(2). With the June 25, 2010, expansion of self-classification eligibility for ENC-U and most mass market items, this should create only

---

[16] Former decontrol note (g) to 5A002 stated the following: (g) *Equipment meeting all of the following:*

1. *All cryptographic capability specified by 5A002.a meets any of the following:*
   a. *It cannot be used; or*
   b. *It can only be made useable by means of 'cryptographic activation';* <u>*and*</u>

2. *When necessary as determined by the appropriate authority in the exporter's country, details of the equipment are accessible and will be provided to the authority upon request, in order to ascertain compliance with conditions described above;*

N.B. 1: See 5A002.a for equipment that has undergone "cryptographic activation."

N.B. 2: See also 5A002.b, 5D002.d and 5E002.b

a need to keep track of key length increases for purposes of determining whether annual self-classification reporting is required.

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 EAR § 740.17(d)(1)(iii). 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 Supp. 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. IMPLEMENTATION OF WASSENAAR 2015 CHANGES FOR NON-CRYPTOGRAPHIC ITEMS. Cat. 5, Part 2 was partially restructured at the Wassenaar 2015 plenary meeting. The primary changes at the multilateral level were to shift certain information security items that were controlled under sub-paragraphs of 5A002.a to newly created ECCNs. For example, non-cryptographic information security items formerly in 5A002.a.4 and a.6 moved to new 5A003, and "cryptanalytic" items formerly controlled under 5A002.a.2 were moved to new 5A004.

3.7. COMPLIANCE WITH ENCRYPTION CONTROLS REMAINS CRITICAL. While reforms since 1996 have dramatically reduced controls over exports of encryption products, the encryption regulations remain incredibly complex. It is critical to take appropriate steps to ensure that companies do not export or facilitate exports of strong encryption products without full compliance with U.S. export controls. New enforcement cases are arising in this area every day, and the enforcement policy of the Commerce Department's Office of Export Enforcement is still evolving. Civil penalties of up to $250,000 per violation can mount up 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. Making clear that

such enforcement risks are not theoretical, Wind River Systems, Inc. settled a voluntarily disclosed enforcement case in October 2014 for $750,000. Settlement documents for this rare encryption enforcement case are available at http://efoia.bis.doc.gov/index.php/component/docman/doc_download/959-e2394?Itemid=. The company made 55 exports of ENC-R software valued at $2.9 million to governments and various end users in China (including some on the Entity List), Hong Kong, Russia, Israel, South Africa, and South Korea. OEE said the company received substantial mitigation credit.

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 § 734.17, or (b) obtain written BIS approval of a different method of distribution that provides similar protections against easy access by foreign nationals and persons outside the United States.

3.8. 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, merging 5X992 Mass Market and 5X002 ENC-Unrestricted categories, so as to eliminate wasted effort distinguishing between them, and removing more of the “virtual ITAR” control vestiges, including as described further in 4.3.6 below. While the October 2008, June 2010, and September 2016 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 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 (now merged into CompTIA) 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://efoia.bis.doc.gov/index.php/component/docman/doc_view/696-license-exception-enc?Itemid=526. A letter signed by members of the RPTAC Encryption Working Group, including this author as Co-Chair for many years, is available on request. The groups have continued providing input.

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.

4.2. LIMITED EAR PROVISIONS ADDRESSING E-COMMERCE. Currently, the EAR explicitly addresses e-commerce in only two places. First, EAR § 734.17 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, and gray areas of the law make exporters uncomfortable. Second, EAR § 758.1(b) (and the Census Foreign Trade Statistics Regulations in 15 C.F.R. § 30.2(d)(3)) exempt intangible exports (via e-mail, downloads, and other electronic transfers) from requirements for exporters to file AES. Prior to September 20, 2016, EAR § 740.13(e)(4) stated 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 …."; however, that provision was removed when the process for making encryption source code publicly available was moved to EAR § 742.15. 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. BIS issued an Advisory Opinion in 2009 confirming this as a generally applicable concept for mass market software. *See* http://www.bis.doc.gov/index.php/forms-documents/doc_download/529-downloads-of-encrypted-software-reviewed-and-classified-as-mass-market.

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 § 734.17 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 § 734.17(c) 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 Country Group E 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, encryption source code and object code derived from published source code is not subject to the EAR, and proprietary software incorporating open source and other "freeware" remain subject to the regulations. EAR § 742.15(b) states that ECCN 5D002 encryption source code (and in EAR § 734.3(b)(2) and Notes) 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 EAR jurisdiction, provided one has submitted written notification to BIS and NSA.

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. The BIS Advisory Opinion dated September 11, 2009 mentioned above also confirmed this approach applies for publicly available mass market software.

4.3.3. ENC Unrestricted Eligible Encryption Software EAR § 740.17(b)(1) and (3). 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 § 734.17 like those for ENC-Restricted EI software. The preamble to 65 *Fed. Reg.* 2492-93 (Jan. 14, 2000) (and certain other amendments) twice said what was then called "retail" encryption software is exempt from Internet download screening requirements, but it also said "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. <u>License Exception TSR Eligible Software EAR § 740.6</u>. 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. <u>NLR and License Exception TSU Eligible Software (EAR § 740.13 Mass Market, Non-EI beta TMP, NLR Based on CCL Classification, EAR99 Items)</u>. 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 Supp. No. 3 to part 732 of the EAR.

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. <u>OFAC General Licenses, Commerce Advisory and Proposed Regulation for Published Software</u>. 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. OFAC noted that, "[a]s events in Iran since last June's [2009 Iranian] Presidential election there have shown, personal Internet-based communications are a vital tool for change."

The exclusion of "published" software from the EAR by EAR 734.7, at that time, did not include software classified under ECCN 5D002 or mass market ECCN 5D992 classified encryption software. Thus, at the time, they were controlled under the CCL and could not qualify as "informational materials" that otherwise would be exempt from OFAC sanctions. EAR § 734.7(c). However, subsequent changes to the EAR in 2011 and 2016 permit both 5D002 and 5D992 items that have been published to be excluded from EAR jurisdiction, subject to compliance with notice requirements. This removed some of the issues relating to limits on downloads.

Prior to those changes, BIS stated in a September 11, 2009, Advisory Opinion 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 and September 2016 rules eliminated many of these issues by releasing publicly available encryption source and object code from EAR jurisdiction, after required notifications.

Note that free patches and updates that can be used only 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, but the regulations remain unclear.

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. However, 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 industry pleading, 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 can inhibit 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. The BIS position on whether access by a foreign national to an IT system with export controlled technology on it was a "release" of such technology was not officially clear until 2016 changes to definitions, in the context of the Export Control Reform. BIS indicated in the preamble to the Federal Register notice that a "foreign person's having theoretical or potential access to technology or software is … not a ''release" because such access, by definition, does not reveal technology or software." 81 *Fed. Reg*. 35586, 35592 (Jun. 3, 2016). Previously, DDTC had taken the position verbally that merely granting access to unsecured technical data equals an export, which interpretation seemed to be embodied in a parallel proposed definitions rule issued in 2015.[17] As of

[17] *See* 80 *Fed. Reg*. 31525, 31535, (Jun. 3, 2015).

early September 2017, DDTC has not finalized its definition of "release," but did issue a follow-up regulation in which it, in the preamble, mirrored the BIS position above, stating, "One commenter asked if theoretical or potential access to technical data is a release. The Department confirms that theoretical or potential access to technical data is not a release. As stated in the preamble to the interim final rule however, a release will have occurred if a foreign person does actually access technical data, and the person who provided the access is an exporter for the purposes of that release." 81 *Fed. Reg.* 62004, 62005 (Sep. 8, 2016). DDTC indicated in the same rule that it anticipates making further changes to the definition of "release" in the ITAR, which hopefully will clearly adopt this position.

These statements indicate that, to enforce a violation, 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 to prevent potential violations, 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 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 four main types of services:

- 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 do present similar compliance issues. BIS has taken the lead in responding to some of the issues raised by cloud computing by issuing a number of advisory opinions and implementing changes to the definition of "export" aimed at public cloud computing, with DDTC coming into the field with a yet-to-be implemented 2015 proposal in the context of Export Control Reform, and OFAC has provided, so far, only one FAQ with any cloud-specific guidance. Thus, this section will focus on EAR compliance issues, 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 three advisory opinions in response to questions from cloud computing service providers, which address these questions primarily in the context of a "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 – which is not always true in the cloud computing environment - 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. Before applying them, exporters should examine the extent to which these underlying premises comport with what in fact is happening in their case.

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).

BIS issued a third advisory opinion on “Cloud-Based Storefronts” on November 13, 2014, which addressed an exporter’s questions about the provision of access to SaaS applications without download of any software. While many viewed the issues raised by the exporter as having been generally addressed in the prior advisories, the 2014 advisory squarely addressed the provision of SaaS access to so-called “License Exception ENC-Restricted” software to “government end-users.” Normally, ENC-Restricted software eligible for the License Exception under EAR § 740.17(b)(2) cannot be exported, reexported, or retransferred to a “government end-user” outside the countries listed in Supp. 3 to EAR Part 740. BIS confirmed that, consistent with its 2009 Advisory Opinion, there would be no “export” of software if there is no download, and thus there is no basis for a license requirement for a non-Supp. 3 “government end-user.”

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 3E001 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 BIS advisory 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.

In addition to these interpretations, BIS (along with DDTC) proposed changes in 2015 to exclude certain transfers of technology or software from the definition of "export," "reexport," and "transfer", based on the use of adequate encryption and security measures to ensure that the data has not been "released" to a foreign national or in a foreign location. BIS implemented these changes in a June 3, 2016 final rule, which became effective September 1, 2016. The rule inserted a new sub-section of the EAR, § 734.18 defining certain "activities that are not exports, reexports, or transfers" under the EAR.

> (a)(5) Sending, taking, or storing "technology" or "software" that is:
> (i) Unclassified;
> (ii) Secured using 'end-to-end encryption;'
> (iii) Secured using cryptographic modules (hardware or "software") compliant with Federal Information Processing Standards Publication 140–2 (FIPS 140–2) or its successors, supplemented by "software" implementation, cryptographic key management and other procedures and controls that are in accordance with guidance provided in current U.S. National Institute for Standards and Technology publications, or other equally or more effective cryptographic means; and
> (iv) Not intentionally stored in a country listed in Country Group D:5 (Supp. No. 1 to part 740 of the EAR) or in the Russian Federation.
>
> Note to paragraph (a)(4)(iv): Data in-transit via the Internet is not deemed to be stored.
> EAR § 734.18(a)(5) (2016)
>
> The regulation also defines "end-to-end encryption:"
>
> (b) Definitions. For purposes of this section, End-to-end encryption means (i) the provision of cryptographic protection of data such that the data is not in unencrypted

> form between an originator (or the originator's in-country security boundary) and an intended recipient (or the recipient's in-country security boundary), and (ii) the means of decryption are not provided to any third party. The originator and the recipient may be the same person.
> EAR § 734.18(b) (2016).

The definition of "end-to-end encryption" proposed in June 2015 had suggested that data encryption had to be uninterrupted as between the originator and recipient. Industry comments pointed out that, to be used effectively, cloud and company IT systems may need to store data in clear text within the security boundaries of a company's servers or within cloud based systems, which should not undermine the ability to use cloud or distributed computing resources, given that the information would remain secured within the system vis a vis outside users.

The FIPS 140-2 standard defines four levels of security, and the definition does not call out any particular level, so presumably FIPS 140-2 Level 1 security or its equivalent would be sufficient to satisfy the requirement. All FIPS 140-2 Levels involve, among other things, use of an "approved algorithm" for bulk data encryption, such as the Advanced Encryption Standard (AES) algorithm defined in FIPS 197, Triple-DES Encryption Algorithm (TDEA) defined in NIST Spec. Pub. 800-67, or the Escrowed Encryption Standard (EES) defined in FIPS 185. There are also requirements for minimum standards for authentication, secure hashing, and random number generation requirements.

Many commercial products already implement these standards, which are effectively a decade old already, but not all commercially available security products have gone through the certification program offered by NIST to confirm that they are FIPS 140-2 compliant, which is more common for products that are marketed to the U.S. Federal Government. Accordingly, the BIS regulation does not require the software or hardware used to be certified as FIPS 140-2 compliant, but rather the items can have equivalent security, to the extent verified by the exporter. It may be necessary for exporters to work closely with IT vendors and their own staff to confirm whether their cloud services are compliant, if indeed they intend to have export-controlled information exported via cloud mechanisms.

That said, the cumulative effect of the prior BIS advisory opinions and this revised definition may still create an environment where a person who places information into the cloud may lack sufficient knowledge with respect to the routing of information by the cloud service provider to be held accountable for a violation, even if the transmission does not meet the end-to-end encryption requirements. Ensuring that the cloud service provider also provides "end-to-end encryption" that complies with the above mentioned definitions may be adding "suspenders" to the "belt" of the advisory opinions when it comes to public cloud computing. On the other hand, it does provide a safe harbor mechanism for compliance that works for some, but by no means all providers and exporters.

The addition of EAR § 734.18 may be of greatest help to companies that use private or hybrid cloud environments, where there is a closer relationship between the provider and the user, and providers may obtain knowledge or have reason to know that there is export controlled technical data or software present on their systems, provided that the cloud service provider can certify FIPS 140-2 or equivalent encryption, and compliance with the "end-to-end encryption" definition. The definitions are also broad enough to apply to in-house IT systems, and create a clearer standard and safe harbor when designing internal technology control programs, and implementing protocols for security of technical data during travel.

4.7.2. ITAR. DDTC's view about a compliant cloud is reflected in an FAQ on its website:

Q: Does saving ITAR controlled technical data on the cloud constitute an export per ITAR § 120.17?

A: A cloud service provider's receipt of effectively encrypted technical data uploaded by the U.S. owner, stored and managed on a cloud service network consisting of only U.S.-based servers, administered only by U.S. persons, and appropriately configured to enable the U.S. technical data owner to control access to such data does not constitute an export under the ITAR.

See http://www.pmddtc.state.gov/faqs/ecr.html#l – Under "Technical Data"

This approach, while giving a nod to encryption, does not go as far as the revised BIS definition, which excludes the movement of encrypted items from the definition of an "export." As discussed above, DDTC proposed similar regulations in 2015that took the same tack as BIS.[18] See 80 *Fed. Reg.* 31525, 31537 (June 3, 2015). The proposal would have added a new section, ITAR § 120.52(d), which excludes from the definition of "export," "reexport," or "retransfer" the routing of technical data or software through the Internet infrastructure of a foreign country, provided that the transmission is subject to "end-to-end" encryption that is secured on equipment that has been certified as compliant with NIST FIPS 140-2 standards, and provided that the data is not stored in a country identified in ITAR § 126.1 or the Russian Federation.

The DDTC proposed definition of "end-to-end encryption" was fundamentally the same as was proposed by BIS in 2015, but differed by requiring equipment and procedures to be certified as compliant with NIST standards, while the BIS rules permit alternative encryption methods that are "similarly effective." This is consistent with Federal Government procurement requirements for IT systems. However, it is unclear whether cloud service providers will be able to consistently confirm that all equipment on which ITAR-controlled technical data resides is NIST-certified, given the intentionally elastic and dynamic characteristics of cloud services.

While these changes were proposed in the context of a broad definitions rewrite for both the ITAR and EAR, DDTC did not publish revisions to its definitions of "export" or "release" on June 3, 2016, but issued only some of its proposed changes that didn't really affect the cloud computing issues. DDTC appears to have been receptive to comments regarding the cloud computing issue. However, we understand that DDTC felt, after reviewing the comments, that a more objective definition was needed that would allow foreign users a clear equivalent to the FIPS 140-2 certification requirement, unlike the BIS rules, which allow exporters to self-certify the equivalence of their encryption measures.

Thus, for now, the ITAR approach to cloud computing remains DDTC's position prior to this proposal, as indicated by the FAQ cited above. Limiting a cloud to use of resources in the United States, administration only by U.S. Persons, and allowing access only to U.S. Persons makes for an expensive and limited use "private" or shared private cloud.

---

[18] DDTC had solicited the advice of the Defense Trade Advisory Group ("DTAG"), which presented a white paper and recommendations on May 9, 2013. The crux of the recommendation was a proposal to re-define "technical data" in ITAR § 120.10 to exclude information encrypted in conformance with a defined or referenced standard, or to create an exemption to licensing requirements for appropriately encrypted technical data. The report and recommendations are available at http://www.pmddtc.state.gov/DTAG/index.html. Subsequently, DDTC and BIS engaged in additional interagency discussions and consultations with industry and the BIS Technical Advisory Committees regarding the potential efficacy of the approach, and both decided to take the approach of excluding encrypted communications from the definition of "export", etc.

The FAQ's inclusion of the vague term "properly encrypted" is perhaps reflective of DDTC's past treatment of the mere ability to access information as sufficient to constitute "release" of technical data or software, not a showing of actual access.[19] That said, as quoted in the beginning of this section, DDTC appeared to back off this "theoretical access" approach in the preamble to its Sep. 8, 2016 rule, indicating that "theoretical or potential access to technical data is not a release." 81 *Fed. Reg.* 62004, 62005 (Sep. 8, 2016). This statement may be practically useful, however, only in a defensive posture where a company unintentionally grants system access to an unauthorized foreign national, since the minute that a foreign national actually does access the controlled data, it is considered an export. In other words, DDTC may have backed off only from its ability to determine a violation to have occurred when the door has been left open to a foreign national, or she has been given a key, but she does not actually enter the room. From a risk management perspective, however, cloud providers and users cannot play fast and loose, and must await the implementation of the encryption related provisions of the proposed DDTC rule before potentially expanding "ITAR-compliant" clouds beyond borders or allowing them to have foreign national administrators.

In light of the recent uptick of foreign-instigated hacking attempts against U.S. defense contractors and government servers, it is unclear whether major companies that are subject to ITAR regulation will embrace the new proposal in practice, despite the requirement to use certified hardware. As discussed above, compliant systems may be limited to a small portion of cloud storage providers, and may not be supportable for SaaS, PaaS, or IaaS systems. It at least provides a safe harbor, and the two proposals represent pragmatic approaches by DDTC and BIS that may be enhanced further by industry comments.

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 Cuba, Crimea, Iran, Sudan, and Syria sanctions, as well as the proliferation of assets blocking sanctions targeted at Specially Designated Nationals (SDNs) and foreign governments.

For example, as reflected in the aforementioned BIS advisory opinions, 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 the user in Iran is an employee or service provider, who is using the SaaS to provide services to the U.S. person, or vice versa.

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-1 (issued May 30, 2013, updated Feb. 7, 2014, http://www.treasury.gov/resource-

[19]One company's announcement in 2014 that DDTC had approved its "tokenization" scheme in a cloud computing context as "ITAR-compliant" created some confusion. "Tokenization" is a structure where a remote user is able to access items stored on a cloud server, but those items do not actually transfer to the remote user's computer. That announcement was followed by a strongly worded clarification by DDTC indicating the company had interpreted the advisory too broadly, and DDTC's opinion had been limited to certain circumstances and conditioned on meeting certain requirements (not well defined), and should not be interpreted as an approval of the technique, usable across-the-board to secure access to ITAR-controlled information/software.

center/sanctions/Programs/Documents/iran_gld1.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-1 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. Note the mention of "cloud" as being covered in OFAC FAQ 441 available at http://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#sud_iran_comms.

> **441. Do the Personal Communications GLs authorize the exportation of fee-based cloud computing services to Iran and Sudan**
>
> Yes. Paragraphs (a)(1) of the Personal Communications GLs authorize the exportation to Iran and Sudan of fee-based cloud computing services incident to the exchange of personal communications over the Internet. In addition, paragraphs (a)(2)(i) and (a)(3) authorize software necessary to enable such services, provided that such software is designated EAR99 or classified by the U.S. Department of Commerce on the CCL under ECCN 5D992.c or, in the case of software that is not subject to the EAR, would be designated EAR99 if it were located in the United States or would meet the criteria for classification under ECCN 5D992.c if it were subject to the EAR. [2-17-2015]

Part of the initial relaxation of sanctions against Cuba, which were also implemented for Sudan at the same time, included the addition of EAR License Exception CCD and OFAC "personal communications" general license to authorize the sale of consumer communications devices. The Ukraine-Related OFAC sanctions also contain a personal communications general license, General License 9, mirrored by EAR § 746.6(a)(1), authorizing the provision of services and software, but not hardware, to the Crimea region of Ukraine. It should be noted that the OFAC sanctions against Syria prohibits the export of services to Syria, but does not contain a similar personal communications general license, which means that the same level of services are not authorized for Syria without a license.

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-1 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. Further, the scope of equipment permitted is limited to consumer devices, and does not include infrastructure items that may be necessary to support the use of such devices on in-country networks. The definitions of what constitutes a permitted consumer device are also not entirely clear, and create gray areas when it comes to certain enterprise-class equipment.

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.

Now that the EAR changes have been implemented, it is possible for service providers to provide certification of compliance with the end-to-end encryption compliance requirements outside of a U.S.-based and administered cloud infrastructure. We anticipate providers will be slow to do so, or may wait until the ITAR changes become effective, as it is frequently difficult for companies to differentiate between ITAR and EAR items, particularly in the defense industry, and there is currently no encrypted "safe harbor" under the ITAR.

4.8. EXPORTERS SHOULD BE VERY CAREFUL ABOUT ASKING 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 has more restrictive requirements for electronic records than paper records, 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

We hope this article sheds light on the difficult application of export controls to technology and software. Further reforms are needed in some areas to avoid theses controls simply being a trap for the unwary. Remember, though, that asking for clarity resulted in the "deemed export rule." However, knowledge of the regulations and tight compliance programs can help reduce troublesome roadblocks to speed bumps in most cases.

BHF/DFO