§ 8.02 Export Controls on Technology

[1]—"Export" Defined

All United States exports are subject to some degree of regulation by the United States federal government.[1] An "export" is any sale, transfer or other movement of a product out of the United States. For regulatory purposes (and as used here), this definition is interpreted very broadly. Exports, for example, are not only sales made by companies engaged in the business of selling products abroad, but include any transfer by a United States citizen or United States-resident entity or alien. Movement out of the country includes not only physical transfer, but also verbal disclosure and data transmission. Products include not only goods such as integrated circuits and software sold abroad, but know-how (incorporated into services or disclosed in a casual conversation, for example) and items brought in carry-on luggage for personal use on a trip abroad. Moving a product out of the country includes transfers made by United States citizens while they are abroad and transfers made to foreign citizens located in the United States.[2]

[a]—Special Information Disclosure Issues

The Export Administration Regulations (EARs) apply the same control framework to both commodities and technology.[3] Technology, however, faces unique export issues to the extent that it may not "physically" be exported or transferred. Two aspects of the export or release of technology are discussed below: distribution on the Internet and exposure to foreign nationals.

[i]—Distribution on the Internet

The Internet is one of the most unregulated communications services today. A communications link for people worldwide, it not only supports the transfer of short messages, but also the transfer and publication of very large quantities of data.

Internet transfers are treated like transfers made through other distribution methods, and information published on the Internet is treated like other

---

[1] Exports are subject to many and complex regulations, and giving counsel with respect to these regulations is a specialty unto itself—this section should be taken only as a primer to the field, and practitioners should only offer counsel after direct reference to the regulations.

[2] See 15 C.F.R. §§ 730.5, 734.2(b). Also see, MacLaren, *Eckstrom's Licensing in Foreign and Domestic Operations/Joint Ventures*, 5-7 (1998).

[3] Technology refers to various forms of technology, software and manufacturing know-how.

methods of publication.[4] For example, an e-mail to a foreign destination is considered an export via facsimile or telephone.[5] The standard of care for all Internet transfer activity is the same standard of care required for all other export activities.[6] Companies should be especially careful about Internet communication between their directors or agents and individuals in restricted countries.

To the extent that a company publishes or distributes on the Internet information or technology that is fully accessible to the public for free,[7] there should be no violation of the Export Administration Regulations.[8] A series of rules and qualifications outlines the parameters for "publicly available" information and technology and should be consulted when conducting activities on the Internet.[9]

When technology may be transferred over the Internet, either in the form of downloading it from a Web site or attaching it via e-mail, companies should be wary of providing information to restricted individuals, companies, and governments. Just as true mailing addresses should be reviewed to check for obvious country restrictions, so too should Internet or e-mail addresses.

[ii]—Disclosure to Foreign Nationals

Another area of unique importance for the potential transfer of technology is that of disclosure to foreign nationals. To a very large extent, United States-based technology firms are conducting research and design activities in areas outside of the United States. When United States-origin technology is released to foreign nationals, an export violation under the EARs may occur.[10] Companies should not worry about violating the EARs when permanent residents and other protected individuals are involved.[11] The export rule, however, is based upon the identity of natural persons and not the

---

[4] See Christensen, *Technology and Software Controls Under the Export Administration Regulations*, 384 (PLI 1997).

[5] *Id.*

[6] *Id.* at 385.

[7] This does not include any Internet service provider charges, cost of software, or other associated computer costs to access the information.

[8] See 15 C.F.R. §§ 734.4(b)(3), 734.7.

[9] See 15 C.F.R. § 734.7.

[10] See 15 C.F.R. § 734.2 (b)(2)-(5).

[11] See 59 Fed. Reg. 13,449. See also, Immigration and Naturalization Act, 8 U.S.C. § 1324b(a)(3). Note that U.S. citizen status may be required under certain conditions such as national security activities.

identity or nationality of the corporate entity, its divisions or parent company.[12]

As previously mentioned, technology can be exported in a variety of ways, including written and verbal communications, electronically recorded media, and visual inspection.[13] To protect themselves against any EAR's violations, exporters should review their technology and consider applying for an export license or qualifying for a license exception. Another option is to apply for a license to release information to all foreign nationals that may learn of the technology.[14]

[2]—Jurisdiction

At least ten federal agencies have jurisdiction over United States technology exports. These agencies include the Departments of Commerce, Defense, Energy, State and Treasury. The primary focus of these agencies is the denial of defense-related technology to enemies or potential enemies of the United States. A secondary focus is the enforcement of embargoes imposed by the United Nations or unilaterally by the United States.

In 1995, to simplify matters, the Department of Commerce was designated as the lead agency for regulating technology exports.[15] The Bureau of Export Administration (BXA) is the part of the Department of Commerce assigned to fulfill the Department's mandate to regulate exports. BXA decisions to allow or to prohibit certain exports are often made only after review and comment from other agencies. For example, the Departments of Defense, Energy and State and the Arms Control and Disarmament Agency have the right to pre-review any export.

[3]—Regulatory Framework

The Export Administration Act of 1979 (EAA) is the legislative authorization for the BXA. It is the most recent law in a line of export-regulating statutes dating back to 1775.[16] To implement statutory requirements, the BXA has promulgated the Export Administration Regulations.[17] While the EAA expired on August 28, 1994, the controls established by the Act and the regulations have since remained in effect by

---

[12] See Christensen, *Technology and Software Controls Under the Export Administration Regulations*, 387 (PLI 1997).

[13] See 15 C.F.R. § 732.2(b)(3).

[14] This includes employees, consultants, attorneys, etc.

[15] Exec. Order No. 12,981. "Administration of Export Controls," 60 Fed. Reg. 62,981 (Dec. 6, 1995).

[16] The Continental Congress outlawed exports to Great Britain in December 1775.

[17] See 15 C.F.R. §§ 730-734. These regulations were restructured and reorganized by the BXA in 1997. See 62 Fed. Reg. 25,451.

virtue of Executive Order 12,294.[18] The regulations establish a framework for the issuance of export licenses by the BXA.

Pursuant to the regulations, the BXA has assigned products to various classifications, and each classification has a unique Export Control Classification Number (ECCN). The entire list of products and ECCNs is referred to as the Commerce Control List (CCL). The BXA also maintains a Commerce Country Chart (the Country Chart) which lists those countries subject to export restrictions, including embargoes. Countries are divided into numbered "tiers," with each higher-numbered tier representing countries subject to more stringent control. By correlating the ECCN for a product with the Country Chart, one can determine whether and how a license can be obtained for a particular export.

The regulations cover essentially any material, technology, software or other item that has or may have a military use. "Technology" is defined as "[s]pecific information necessary for the 'development,' 'production,' or 'use' of a product."[19] In determining the ECCN for a product, each commodity, software, technology or other component of the product or used in the manufacture of the product must be taken into consideration.[20] Even imported products, if they incorporate restricted technology, are subject to controls.[21]

[4]—Export Restrictions[21.1]

[a]—Generally

The regulations stipulate that, unless there is a specific exemption in the regulations, or unless an export license is obtained from the BXA, no exporter may do any of the following:[22]

(1) Export any item subject to the regulations to another country, or reexport any item of United States origin, if the item is controlled as indicated in the applicable ECCN and the country of destination requires a license as set forth in the Country Chart;

---

[18] Exec. Order No. 12,294, 59 Fed. Reg. 43,437 (1994).

[19] 15 C.F.R. § 772.

[20] A frequent component of advanced technology products and services is encryption technology. While export regulation of encryption technology was significantly relaxed beginning in January 2000, certain controls remain. See § 8.02[11] *infra*.

[21] See 15 C.F.R. § 730.5(b).

[21.1] See § 8.02[11] *infra* for a discussion of export controls over encryption technology.

[22] See 15 C.F.R. § 736.2. Note that country-specific controls change relatively frequently. See 15 C.F.R. § 738.

(2) Export or reexport any foreign-made commodity, software or technology;

(3) Export or reexport to certain destinations an item if it is the direct product of certain technology, software or plants subject to national security controls;

(4) Take any action prohibited by a denial order;

(5) Export or reexport for certain end-uses or to certain end-users;

(6) Export or reexport to Cuba, Libya, North Korea, Iran or Iraq;

(7) Finance, contract, service, support, or transport any product, service or technology that the exporter knows will assist in certain proliferation activities;

(8) Export an item through Albania, Armenia, Azerbaijan, Belarus, Bulgaria, Cambodia, Cuba, Estonia, Georgia, Kazakhstan, Kirghizstan, Laos, Latvia, Lithuania, Mongolia, North Korea, Russia, Tadzikistan, Turkmenistan, Ukraine, Uzbekistan or Vietnam;

(9) Violate a license, a license exception or an order;

(10) Export or reexport or otherwise service any item if the exporter has knowledge that a violation of the regulations, the Act or any order, license, license exception or other authorization has occurred, is about to occur, or is intended to occur.

While the scope of the regulations is far-reaching, only about 4% of the annual dollar value of United States exports end up requiring an export license.[23]

As noted above, what constitutes an "export" for purposes of the regulations is very broad. The regulations also govern "reexport," which is the export of products to one foreign country with the intent of subsequent shipment to another foreign country. There are also United States addresses that are used as "drop-off" destinations—way stations for eventual shipment to foreign countries.

Exporters are not required to conduct their own investigation of each destination address in order to determine whether it is a drop-off address or part of a reexport scheme. However, an objective reasonableness standard is applied to whether an exporter knew or should have known that shipment to a particular destination would likely result in a prohibited export or one requiring a license. To assist exporters in making such assessments, BXA has published a list of "red flag indicators" of what to look for in determining whether those customers who are participating are involved in illegal export schemes.[24] BXA also maintains lists of known drop-off and re-port destinations. Exporters are required to refer to these lists before making any shipment.

---

[23] Bureau of Export Administration, "History of Export Controls" (1999).

[24] This list of red flag indicators is included in "Element 3" of the Export Management Guidelines found at Appendix C *infra*. See § 8.02[9] *infra*.

[b]—High Performance Computers (HPCs)

In February 1998, BXA issued a regulation requiring advance notification of all exports and reexports of certain high-performance computers (HPCs) from the United States to countries listed in "Tier III" of the BXA Country Chart, including China, India, Israel, Russia and Vietnam. This regulation implements provisions of the 1998 National Defense Authorization Act. HPCs are defined as computers with processor speeds between 2,000 and 7,000 million theoretical operations per second (MTOPS).[25] As such, HPCs represent an intermediate class of computers between personal and commercial-grade computers, which are subject to very few export restrictions, and supercomputers, the export of which to Tier III countries always requires an export license.[26]

A United States exporter or reexporter must submit a notice to BXA before making any shipment of an HPC to a Tier III country. This notice must describe the proposed sale or a series of related sales, including the purchaser's identity. BXA refers all notices to the United States Departments of Defense, Energy and State, as well as the Arms Control and Disarmament Agency. If no objections are raised by these agencies, the shipments may take place without a license. Otherwise, the notice will automatically assume the status of an export license application and will be handled accordingly by the BXA.

BXA must perform post-shipment verifications on all shipments of computers with processor speeds in excess of 2,000 MTOPS to Tier III countries. Consequently, each United States exporter or reexporter of such computers must, within thirty days after shipment, provide a written report to BXA that includes specified end-user information.

Illustrating the pitfalls of regulating rapidly changing technology, about one year after these regulations went into effect, computer industry leaders testified before Congress that cost-performance advancement may cause the number of HPC notifications to rise from 800 during 1998 to 300 per day by 2000.[27] This volume of requests would severely tax BXA's resources; excessive delays will also put United States manufacturers at a significant disadvantage relative to Japanese and European exporters, which are subject to no such restrictions. As the cost of computers capable of such sensitive tasks as designing and modeling nuclear weapons decreases, United States legislators and regulators will need to re-assess the current paradigm that weapons proliferation can be reduced and national security increased by means of restricting United States exports.

---

[25] 15 C.F.R. § 742.12.

[26] By way of reference, in mid-1999, leading-edge supercomputers are capable of approximately one billion MTOPS.

[27] "U.S. May Lose Computer Exports," Reuters (March 17, 1999).

[c]—Wassenaar Arrangement

The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies establishes a multilateral framework for the global regulation of the export of militarily sensitive technologies. The Wassenaar Arrangement was approved by the thirty-three co-founding countries in July 1996 and is the successor to the Coordinating Committee for Multilateral Export Controls (COCOM) regulatory regime in effect during most of the Cold War.

The Wassenaar Arrangement went into effect in September 1996 with an organizational office in Vienna, Austria. This organization promulgates guidelines, regulations and reporting requirements and maintains lists of technologies that are or can be used in the manufacture of conventional weapons. The intent of this activity is to ensure that sensitive technologies do not contribute to the development or enhancement of military capabilities that cause international destabilization. Member countries implement these regulations by means of their own national policies (some with more effect than others). The EARs and the Commerce Control List in effect represent the United States implementation of the Wassenaar Arrangement.

[5]—Exceptions

Exceptions to license requirements are based on the product, the ultimate destination, the end-use and the end-user. If more than one exception is available, the exporter can select the exception that is the most broad and permissive. Subject to certain limitations, license exceptions are available for exports in the following circumstances:[28]

(1) Temporary import, export and reexport of commodities and software;

(2) Servicing and replacement of parts and equipment;

(3) Export and reexport of gift parcels;

(4) Export and reexport of operation technology and software, sales technology, software updates and "mass-market" software.[29]

[6]—Export License Types and Term

Licenses can be applied for on BXA forms or, with prior BXA approval, electronically. Export licenses are either for a specific transaction, a specific series of transactions, or are Special Comprehensive Licenses (SCLs) which can be used for multiple exports and reexports.

---

[28] 15 C.F.R. § 740.

[29] Note that the exception for mass-market software does not include any such software containing 16-bit (or more advanced) encryption technology. 15 C.F.R. § 740.13(a). See N. 20 *supra* .

Licenses typically expire within twenty-four months of the date of grant. If the BXA learns of a license violation (whether from the exporter or by any other means) or believes that a violation is about to occur, the BXA can unilaterally revise, suspend or revoke the license, in whole or in part, without any prior notice to the exporter.

In order to use an SCL, an exporter must have in place an internal audit and control program to ensure compliance with the SCL.[30] Self-reporting of violations is encouraged, and requests to participate in unsanctioned foreign boycotts are required.[31] In no event can a product subject to an SCL be exported or reexported to the following countries: Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria.

[7]—Application Process

To expedite review, a separate license application should be filed for each product type (whether the application is for a specific transaction or for an SCL), although not necessarily for each ECCN. Applications are reviewed by different offices within the BXA and are usually reviewed by other agencies as well. Reviewers tend to specialize in product types, so an application covering more than one type will require time-consuming coordination and a final determination will not be given until after the last reviewer has finished.

Applications for export licenses can be accepted or denied in whole or in part, unless the applicant has requested that the application be either wholly approved or wholly denied. Applications missing required information or which are otherwise not in conformance with regulatory requirements (which defects cannot be corrected with a phone call) will be returned by the BXA without action (i.e., without any approval or denial) and must be resubmitted for approval.

Corrected and correctly completed export license applications will be entered into the BXA's computerized database. Any application that has been entered into the database will be either decided upon or referred to another agency within ninety days. Applicants can check the status of their applications using a touch-tone telephone by accessing the BXA's automated voice response system.[32]

[8]—Denial and Appeal

If the BXA decides to deny any application for an export license, it will send the applicant a written notice of its intent to deny the application. Unless

---

[30] See § 8.02[9] and Appendix C *infra*.

[31] Reporting is encouraged, for example, in the Export Management Guidelines found at Appendix C *infra* (Element 6, Notification**)**. Boycott request reporting requirements are found in 15 C.F.R. § 760.5.

[32] This system is referred to as "STELA," which stands for System for Tracking Export License Applications. The telephone number is (202) 482-2752.

the applicant responds to this notice within twenty days of the date of the notice, the denial will become final forty-five days after the date of the notice. Any notice of intent to deny an application will contain the following information:

(1) The statutory and regulatory basis for denial;

(2) Any specific considerations that led to the decision to deny the license application;

(3) Any modifications or restrictions to the license application which would cause the BXA to reconsider the application;

(4) The name of a BXA representative whom the applicant can call in order to discuss the application; and

(5) The right of the applicant to appeal a final denial, which appeal must be initiated within forty-five days after the date the denial becomes final (see above).

[9]—Internal Compliance Program

BXA, in response to industry requests, developed a prototype Export Management System (EMS), intended to serve as a model for companies in setting up internal EAR compliance programs. The EMS is offered by BXA as an optional program that each company can consider establishing to ensure that their exports and export decisions are consistent with the EAR.[33]

[10]—Penalties

Exporters may face administrative, civil and criminal penalties for failure to comply with the Export Administration Regulations. Section 764 of the Code of Federal Regulations discusses unlawful conduct and sanctions of the EARs.[34] Unlawful acts may include both *mens rea* and *actus reus* elements,[35] but unlawful conduct on its face may also result in penalties.[36]

Exporters may face several administrative penalties, the most severe of which is the denial of export privileges.[37] Civil fines may range from $10,000

---

[33] A detailed description of EMS is found at Appendix C *infra*.

[34] See 15 C.F.R. § 764.

[35] "Mens rea" refers to an element of criminal responsibility consisting of a guilty mind or a wrongful purpose. "Actus reus" means a wrongful act, which, when combined with the mens rea stste of mind, makes the actor criminally liable. *Black's Law Dictionary* (6th ed. 1990).

[36] See 15 C.F.R. § 764..

[37] See 15 C.F.R. § 764.3(2). See also, 15 C.F.R. § 764.3(3), Exclusion from Practice, which can sanction attorneys, accountants, consultants or other representatives for any license application before the Bureau of Export Administration.

to $100,000.[38] Criminal penalties include monetary fines of up to five times the value of the export or $50,000, whichever is greater, and up to five years of imprisonment, or both.[39] Corporations may face even larger fines.[40]

[11]—Encryption Technology

[a]—Introduction

A substantial revision to the Export Administration Regulations applicable to encryption technology was promulgated by the Bureau of Export Administration on January 14, 2000.[41] This revision was made in response to the encryption export policy announced by the White House on September 16, 1999 and in order to implement revisions to the Wassenaar Arrangement made in 1998.[42]

[b]—Encryption Technology Explained

Encryption is the process of transforming data (text, graphics, computer programs, etc.) into a code that is useful only to intended recipients. Current computer-based encryption technology is a process by which elements of data, such as characters in text or pixels in a graphic, are assigned numeric or other representational equivalents. ("A" could be assigned the number "1," "B" could be represented by "2," and so on.)[43] These equivalents are then converted into another set of data elements by application of a mathematical formula (also known as a "hashing algorithm") that uses a password or "key." (If the hashing algorithm was addition and the key was the number "3," for example, the letter "A," which had initially been assigned the number "1" would be converted to "4," "B" would become "5," and so on.) The resulting, encrypted data is also known as cipher text. In order to decrypt cipher text, the intended recipient must also possess a password or key. In the example above, the cipher text would be meaningless to the recipient, unless she

---

[38] 15 C.F.R. § 764.3(a)(1).

[39] 15 C.F.R. § 764.3(b)(2)(i).

[40] 15 C.F.R. § 764.3(b)(2)(ii).

[41] 15 C.F.R. Parts 734, 740 *et al.* (65 Fed. Reg. 2492).

[42] The announced policy rests on three principles: (1) a technical review of encryption products in advance of sale; (2) a streamlined post-export reporting system; and (3) the establishment of a process for pre-transaction review of exports of strong encryption products to foreign governments. The Wassenaar Arrangement is discussed in § 8.02[4][c] *supra*.

[43] This is a very complex technology, with many variations, not all of which fit precisely within the boundaries of this description. Nevertheless, this description, with its introduction of key terms, is sufficient background to enable understanding of the regulations governing export of encryption technology.

possessed the key (the number "3") and knew or deduced the hashing algorithm.

Devising ever more complex algorithms and keys has been the subject of increasing effort throughout recorded history.[44] Currently, there are two types of encryption in commercial use: Symmetric encryption and asymmetric encryption. (Asymmetric encryption is also known as "public key encryption" or "Diffie-Hellman encryption.")[45] Symmetric encryption requires that the same key be used both to encrypt data and to decrypt it. (The key of the number "3," in the example above, used both to encrypt and to decrypt the data, is an example of symmetric encryption.) Asymmetric encryption uses two keys—a publicly available encryption key and a decryption key known only to the intended recipient of cipher text.

Cracking (i.e., deciphering without the cooperation of the owner) hashing algorithms is a time-consuming business. Interoperability is also a concern. Both these factors favor use of time-tested algorithms. The most common industry practice is, therefore, to use readily available, even public domain, algorithms and to invest most effort in maintaining secure, controlled access to the keys. The best-known symmetric hashing algorithm is DES, which stands for Data Encryption Standard. This public domain algorithm was invented in 1975 and standardized for commercial use in 1981 by the American National Standards Institute (ANSI). The best known asymmetric algorithm is probably RSA.[46] Different algorithms also use keys of different sizes or lengths. With digital (i.e., computer-based) encryption, the size of the key is determined in bits.[47] Given a sound hashing algorithm, the longer the key, the more secure the cipher text and the more time and processing power required to encrypt and decrypt. Most algorithms are able to handle keys of only one size. DES, for example, uses 56-bit keys. Encryption using keys of a given length is often generically referred to by that key length, such as "56-bit encryption," for example, a term that would include DES.

Asymmetric algorithms are currently the most popular means of sending encrypted data over the Internet. RSA, for example is incorporated into both Microsoft Corporation's Internet Explorer™ and Netscape Communications Corporation's Navigator™ Web browsers. The principal technical challenge

---

[44] Encryption has been traced back to ancient Egyptian hieroglyphics and Mesopotamian tablets dating before 1500 B.C.

[45] Asymmetric encryption was invented in 1976 by Wheatfield Diffie and Martin Hellman.

[46] RSA was patented by Ronald L. Rivest, Adi Shamir and Leonard M. Adleman in 1983.

[47] A bit is the smallest unit of measure of data. It can have two possible values: zero or one. A character, such as the number "3" (the key in the example above), requires eight bits' worth of data capacity for almost all modern computers. A byte, the most common measure of data, consists of eight bits and is therefore equivalent to one character.

of Internet use of asymmetric algorithms is the need first to obtain an intended recipient's (public) encryption key. This exchange of encryption keys is often handled by particular software applications and service providers internally (i.e., without reference to generally available "global" key registries) for their particular users and customers. Emerging technologies, such as Lightweight Directory Access Protocol (LDAP), should in the future enable virtually any Internet user to obtain public keys for any other Internet user, regardless of the particular hardware and software used to maintain such information.

[c]—Changes to Export Regulatory Framework

Since January 14, 2000, retail encryption commodities and software (RECS) of any key length can be exported, after a one-time technical review and without a license, to non-governmental end users in any country other than the seven state supporters of terrorism.[48] RECS consists of widely available products used for any purpose, including encryption key exchange infrastructure, e-commerce, client-server applications and software subscriptions. In particular, RECS consists of products and product components meeting all of the following criteria:

- Are generally available to the public: (1) sold in tangible form through independent retail outlets; (2) specifically designed for individual consumer use and sold in tangible or intangible form; or (3) sold in large volume without restriction through mail order transactions, electronic transactions or telephone call transactions;
- Cryptographic functionality has not been modified or customized to customer specification and cannot be easily changed by the user;
- Do not require substantial support for installation and use; and
- Do not consist of network infrastructure products such as high-end routers or switches designed for large-volume communications.

The Bureau of Export Administration of the Department of Commerce (BXA) determines which products are categorized as RECS by means of a pre-export technical review.[49] Products that are functionally equivalent to products classified by BXA as retail (the "R" in RECS) will also be classified as RECS. All encryption software other than publicly available source code must be submitted to such technical review.[50] A copy of any such source

---

[48] 15 C.F.R. § 740.17(a)(3). "RECS" is the author's acronym and has not (yet) entered widespread use. These "bad boy" states are Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria. Restrictions on these seven nations remain in place. Exports to foreign government end users will still require a license.

[49] See § 8.02[3] *supra* for a more general discussion of BXA and the regulation of technology exports.

[50] 15 C.F.R. § 740.13(e)(1).

code, or the Internet address where such source code can be found, must be provided to BXA prior to the initial export thereof.[51] While it is still illegal to export knowingly either RECS or such source code to the seven state supporters of terrorism, simply making such items available for download on the Internet does not constitute "knowledge" of any resulting download to destinations in those nations.[52] There are no restrictions on providing assistance to foreign persons in the use of such source code, and foreign-made products using such source code are not subject to any technical review or notification requirements.[53]

A person submitting product containing encryption technology to BXA for technical review can begin to export the product thirty days after such submission, unless the person first hears from BXA to the contrary.[54] Once a product is categorized as RECS, a subsequent upgrade consisting of only an increase to key length or key exchange technology can be exported upon prior notice to BXA comprised of a letter from a corporate official of the exporter certifying that there is no other change to cryptographic functionality.

Post-transaction reporting of exports of encryption technology is no longer required for the following:[55]

- RECS;
- finance-specific products;
- export to a United States subsidiary;
- exports to or from a United States financial institution, its subsidiaries, affiliates, customers or contractors for banking or financial operations;
- any encryption technology using a symmetric key of 64 bits or less;
- products made available through free or anonymous download.

All other exports of encryption technology must be reported to BXA semi-annually. Such reports must contain the information called for by Section 740.17(g)(2) of the Code of Federal Regulations.

---

[51] Such notification can be e-mailed to BXA at crypt@bxa.doc.gov. Posting on the Internet will, for purposes of this rule, be considered an effective "export" because of the unrestricted access such posting allows.

[52] This rule change is in response to Bernstein v. United States Department of Justice, 176 F.3d 1132 (9th Cir. _1997), in which the Ninth Circuit Court of Appeals found that then-existing regulations purporting to restrict a posting on the Internet of encryption software was in violation of the First Amendment.

[53] 15 C.F.R. § 744.9.

[54] 15 C.F.R. § 740.17(e). Any such request must comply with the guidelines found in Supplement No. 6 to Part 742 of the Code of Federal Regulations "Guidelines for Submitting a Classification Request for Encryption Items."

[55] 15 C.F.R. § 740.17(g)(1).

The European Union continues to move toward making encryption technology freely tradeable among member and other, specified countries. It is the stated policy of the Clinton administration that United States firms will not be disadvantaged by any such elimination of EU controls, which means that remaining controls over United States export of such technology could in such event be further weakened or eliminated altogether.[56]

[56] Paragraph 5 to background information appearing at 65 Fed. Reg. 2494.