[iii]—International Developments

In 1996, the United Nations Commission on International Trade Law (UNCITRAL) adopted legal guidelines to expand the recognition of electronic signatures as valid signatures. UNCITRAL has recommended that governments "review legal requirements of a hand-written signature or other paper-based method of authentication on trade related documents with a view to permitting, where appropriate, the use of electronic means of authentication."[48]

[5]—Introduction to Export Regulations

One issue in the use of cryptography in Internet transactions is that the United States regulates the export of cryptography, as incorporated in products or otherwise.[49] One of the reasons for export restrictions on encryption software is that if the software were used by an enemy of the United States, then United States agencies, including the Central Intelligence Agency and the National Security Agency, might have difficulty decoding potentially hostile messages. This could hinder intelligence efforts. Because United States companies havecomplained that cryptographic regulations hamper their ability to compete in the global market, the United States government has modified the relevant regulations several times. It is important for an entity conducting business on the Internet to have at least a basic understanding of how the United States regulates the export of encryption and the challenges that the relevant regulations have raised.

---

[48] Official Records of the General Assembly, 50th Sess., Supp. No. 17 (A/50/17) (1996). Article 7 of the UNCITRAL Model Law on Electronic Commerce defines "signature" as follows:

> "(1) [w]here the law requires a signature of a person, that requirement is met in relation to a data message if:
>
> "(a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and
>
> "(b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.
>
> "(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature."

A Model Law on Electronic Signatures, refining the earlier Model Law on Electronic Commerce, was adopted by the Commission on July 5, 2001. See http://www.uncitral.org/english/texts/electcom/ml-elecsig-e.pdf.

[49] As an alternative to engaging in transactions through the Internet with cryptography, a company can avoid encryption issues by leasing private phone lines from the telephone company and allowing access to these lines only to authorized customers. However, setting up a network of dedicated lines can be expensive. Encryption software enables start-ups and smaller companies to have world-wide exposure, with minimal expense.

Until December 30, 1996, computer software and equipment containing any encryption functionality were classified as munitions, and their export was regulated by the Department of State under the International Traffic in Arms Regulations (ITAR).[50] On that date, the responsibility for nonmilitary cryptography regulation[51] was transferred to the Department of Commerce Bureau of Export Administration (BXA).[52] In April 2002, the Department of Commerce adopted a final regulation changing the name of the BXA to the Bureau of Industry and Security (BIS).[53] The BIS develops and applies the Export Administration Regulations (EAR).[54]

In a continuing effort to liberalize United States encryption policy, the EAR has been modified several times.[55] The government's encryption regulations have, however, been subject to continuing constitutional challenge.[56] Due to the rapid changes in this area, exporters

---

[50] 22 C.F.R. Parts 120 *et seq.*

[51] The ITAR was amended to exclude nonmilitary cryptography from its jurisdiction. See 22 C.F.R. § 121.1, Category XIII (1999). The ITAR continues to regulate exports of "encryption products specifically designed, developed, configured, adapted, or modified for military applications (including command, control, and intelligence applications)." Memorandum on Encryption Export Policy, 32 Weekly Comp. Pres. Doc. 2397 (Nov. 15, 1996).

[52] Exec. Order No. 13026 (Nov. 1996) (effective Dec. 30, 1996).

[53] 67 Fed. Reg. 20630 (April 26, 2002), 15 C.F.R. Ch. VII.

[54] 15 C.F.R. Parts 730 *et seq.* The most recently updated version of the EAR is available at http://w3.access.gpo.gov/bis/ear/ear_data.html (visited Jan. 28, 2003). References to the EAR in the following discussion are to the updated version available on the GPO site as of the dates indicated in the individual footnotes; dates of update of individual sections referenced in the footnotes refer to the date of revision of the Part of the EAR in which the section appears (as shown in the version available on the GPO site), unless otherwise specifically noted.

[55] The most recent major changes in the EAR provisions on encryption technology were adopted in a June 6, 2002, Final Rule, 67 Fed. Reg. 38855 (June 6, 2002). A chronological list of all Federal Regulations amending the EAR from 1996 to the present is available at http://w3.access.gpo.gov/bis/fedreg/ear_fedreg.html (visited Feb. 3, 2003).

[56] The government's regulation of cryptography was found to be an unconstitutional prior restraint on free speech in Bernstein v. United States Department of State, 945 F. Supp. 1279 (N.D. Cal. 1996) (under the then-current ITAR), *superseded* 974 F. Supp. 1288 (N.D. Cal. 1997) (same result under the original EAR), *aff'd* 176 F.3d 1132 (9th Cir. 1999), *opinion withdrawn, reh'g en banc granted* 192 F.3d 1308 (9th Cir. 1999), *dismissed and remanded* No. 97-16686, D.C. No. C-97-0582 MHP (April 11, 2000) (remanded for reconsideration in light of the Jan. 14, 2000 amendments).

A similar result was obtained in Junger v. Daley, 8 F. Supp.2d 708 (encryption not entitled to First Amendment protection), *rev'd and remanded* 209 F.3d 481 (6th Cir. 2000) (encryption entitled to First Amendment protection; remanded to determine whether, under the amended EAR authorizing Web site posting, Junger is in a position to bring a facial challenge).

See also, Karn v. United States Department of State, 925 F. Supp. 1 (D.D.C. 1996), *remanded* 1997 U.S. App. LEXIS 3123 (D.C. Cir. Jan. 21, 1997) (*per curiam*) (remanded for consideration of reviewability and merits under the Administrative Procedure Act; did not reach the constitutional question).

are advised to seek the advice of experienced counsel to determine the most up-to-date applicable restrictions.

[a]—Scope of the Export Administration Regulations

The phrase "subject to the EAR" is used ". . . to describe those commodities, software, technology, and activities over which the Bureau of Industry and Security . . . exercises regulatory jurisdiction under the EAR . . . ."[57] *Items* subject to the EAR include: (1) all items in the United States and those items moving through the United States while being transported from one foreign country to another; (2) all items of United States origin wherever located in the world; and (3) all United States-origin parts, components, materials, or other items in amounts exceeding certain *de minimis* levels.[58]

The EAR also enumerates those items that are not subject to the EAR, including certain publicly available technology and software[59] and items whose export or reexport is exclusively controlled by other United States government departments and agencies for reasons of national security or foreign policy.[60]

In addition, the EAR sets forth those *activities* that are subject to the EAR, including activities of United States persons related to the proliferation of missile technology or chemical or biological weapons, activities of United States and foreign persons prohibited by any EAR-issued order, and technical assistance by United States persons with respect to encryption commodities or software.[61]

[b]—The Definition of "Export" and "Reexport"

The EAR applies to both the *export* and *reexport* of items and services. The scope of the term "export" varies, depending on the item

---

[57] 15 C.F.R. Part 772.1 (revised Aug. 29, 2002) (cross-referencing § 734.2(a) of the EAR).

[58] A complete list of items subject to the EAR is located at 15 C.F.R. § 734.3(a) (revised June 6, 2002). For the rules on calculating *de minimis* values and their implications, see 15 C.F.R. § 734.4 and 15 C.F.R. Part 734, Supp. No. 2 (revised June 6, 2002). *Id.* § 734.4(b) contains provisions that limit *de minimis* treatment of encryption commodities, software and technology.

[59] 15 C.F.R. § 734.3(b)(3) (revised June 6, 2002). This exclusion does not apply to encryption software, which is defined as "[c]omputer programs that provide capability of encryption functions or confidentiality of information or information systems . . ." and includes ". . . source code, object code, applications software, or system software." *Id.* Part 772 (revised June 6, 2002). Publicly available encryption software does not fall under this exclusion from the EAR, but such software may be eligible for an exception from the license requirements of the EAR. See discussion at § 8.05[5][iii] *infra*.

[60] 15 C.F.R. § 734.3(b)(1) (revised June 6, 2002). These agencies include the Department of State; the Treasury Department, Office of Foreign Assets Control; the U.S. Nuclear Regulatory Commission; the Department of Energy; and the Patent and Trademark Office.

[61] *Id.* § 734.5 (revised June 6, 2002).

or service being exported. As a general rule, export "means an actual shipment or transmission of items subject to the EAR out of the United States, or release of technology or software subject to the EAR to a foreign national in the United States . . . ."[62] When applied to technology or software (with the exception of encryption software), export includes the release of technology or software subject to the EAR in a foreign country or the release of technology or source code subject to the EAR to a foreign national.[63]

When the item to be exported is encryption-source or object-code software, the definition of "export" under the EAR includes "[a]n actual shipment, transfer, or transmission out of the United States" or "[a] transfer of such software in the United States to an embassy or affiliate of a foreign country."[64] In addition, if the export of the encryption-source or object-code software is controlled as "encryption software," the definition of "export" is expanded to include "downloading, or causing the downloading of, such software to locations (including electronic bulletin boards, Internet file transfer protocol, and World Wide Web sites) outside the U.S., or 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, unless the person making the software available takes precautions adequate to prevent unauthorized transfer of such code."[65]

---

[62] 15 C.F.R. § 734.2(b)(1) (revised June 6, 2002). Under the EAR, an "item" is defined as "commodities, software, and technology." *Id.* Part 772 (revised Aug. 29, 2002). A "commodity" is defined as "[a]ny article, material, or supply except [non-encryption] technology and software." *Id.* "Software" is defined as "[a] collection of one or more 'programs' or 'microprograms' fixed in any tangible medium of expression." *Id.*

[63] 15 C.F.R. § 734.2(b)(2) (revised June 6, 2002).

[64] *Id.* § 734.2(b)(9)(i) (revised June 6, 2002).

[65] *Id.* § 734.2(b)(9)(ii) (revised June 6, 2002). These precautions "shall include 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 . . . ;"
>
> "(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 Export Administration Regulations, 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

The EAR defines "reexport" as an ". . . actual shipment or transmission of items subject to the EAR from one foreign country to another foreign country; or release of technology or software subject to the EAR to a foreign national outside the United States . . . ."[66] When applied to technology or software, reexport includes the release of technology or source code subject to the EAR to a foreign national of another country, except those lawfully admitted for permanent residence.[67]

[c]—Classifying an Item or Service

The BIS controls the export of nonmilitary software and technology.[68] For export to be permitted by the BIS, either a license must be obtained or a license exception must apply. The applicant must first classify the item or service under the EAR to determine what license requirements and exceptions exist for the item or service.[69] The most reliable method of obtaining such an Export Control Classification Number (ECCN) is to submit an official classification request to the BIS.[70]

---

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."

Id. § 734.2(b)(9)(iii).

[66] *Id.* § 734.2(b)(4) (revised June 6, 2002).

[67] 15 C.F.R. § 734.2(b)(5) (revised June 6, 2002). "Release" is defined as either the visual inspection of U.S.-origin equipment or facilities by a foreign national, oral exchanges of information abroad or in the United States, or the application of technical experience or personal knowledge acquired in the United States to situations abroad. *Id.* § 734.2(b)(3) (revised June 6, 2002).

[68] For military-purpose software and technology, a would-be exporter must seek the approval of the Department of State, Office of Defense Trade Controls. The process for making such an application is set forth in detail in the ITAR, 22 C.F.R. §§ 120 *et seq.*

[69] Generally, a license is required for the export of any item or service over which the BIS has jurisdiction. The remainder of this section assumes that the item at issue has fallen under the export controls of the BIS.

[70] The application form for an official classifications request, form number BIS-748P, may be requested by phone at (202) 482-4811, or by fax at (202) 219-9179, or otherwise as described at http://www.bxa.doc.gov/factsheets/facts4.htm (visited Jan. 29, 2003). Directions for completing this form can be found at 15 C.F.R. § 748.3 and in Supp. No. 1 to Part 748 (both revised June 6, 2002). Other ways of obtaining an ECCN include contacting the manufacturer, producer or developer of the item or service in question who may know the ECCN by virtue of prior exports of the same item or service or having someone familiar with the item or service consult the EAR to determine the ECCN. However, these methods are less reliable than submitting a request to the BIS. Failure to classify an item or service properly without the assistance of the BIS does not relieve an exporter of its obligation to obtain an export license if one is required under the EAR. 15 C.F.R. § 732.3(b)(1) (revised Nov. 25, 2002).

Determining the ECCN of an item or service using the EAR requires use of the EAR's Commerce Control List (CCL), which sets forth detailed descriptions of items and services.[71] Next to each item and service listed in the CCL is a corresponding ECCN.[72] If no ECCN applies to a specific item or service, then the item or service is classified as EAR99, which is a "catch-all" for items or services not specified in the CCL.[73] The practical effect of an EAR99 classification is that the EAR99 item may be exported without an export license or applicable License Exception. The EAR99 item's export is still subject to the EAR, however.[74] Thus, the General Prohibitions described below should be reviewed before any such item is shipped. As with all other items exported under the EAR, EAR99 items may not be sent to any individual or entity that is the subject of a denial order.[75]

[i]—Classification of Encryption Items

The ECCNs for encryption items requiring a license or a license exception are 5A002 (encryption commodities), 5D002 (encryption software), and 5E002 (encryption technology).[76] The ECCNs for encryption items that are not controlled under the foregoing ECCNs (and, therefore, in general do not require a license for export or reexport but may require notification to or a review by BIS) are 5A992 (encryption commodities), 5D992 (encryption software), and 5E002 (encryption technology).[77] Provisions in various license exceptions set out in Part 740[78] of the EAR and control policy provisions in Part 742,[79] read together with other parts of the EAR, determine what particular encryption items fall within the respective ECCNs, and the extent to which the export and reexport of such items is controlled.

---

[71] The CCL is located at 15 C.F.R. Part 774, Supp. No. 1 (revised Sept. 23, 2002).

[72] *Id.* A review of the CCL should be made in each instance to ensure that the proper ECCN is chosen.

[73] 15 C.F.R. § 732.3(b)(3) (revised Nov. 25, 2002).

[74] 15 C.F.R. § 732.3(d)(5) (revised Nov. 25, 2002).

[75] See 15 C.F.R. § 732.3(g). The standard terms of denial orders are set out in 15 C.F.R. Part 764, Supp. No.1. p. 8-56. All denial orders are published in the Federal Register and the Denied Persons List is available at http://www.bxa.doc.gov/DPL (visited Jan. 31, 2003).

[76] See 15 C.F.R. Part 774, Supp. No. 1.

[77] *Id.*

[78] The license exceptions that pertain expressly to encryption items are those in 15 C.F.R. § 740.8 (Key Management Infrastructure (KMI)), *id.* § 740.13 (Technology and Software—Unrestricted (TSU)), and *id.* § 740.17 (Encryption Commodities and Software (ENC)). See further discussion at § 8.05[5][g][iii] *infra*.

[79] See 15 C.F.R. § 742.15, the control policy provisions applicable to "Encryption Items."

[ii]—Retail and Mass-Market Encryption Commodities, Software and Components[80]

Certain encryption items controlled under ECCNs 5A002 and 5D002 qualify for treatment as "retail" encryption commodities under License Exception ENC.[81] Retail encryption commodities, software, and components are products available to the public, containing low-level encryption sold in tangible form through retail channels, designed for individual consumer use and sold or transferred in tangible or intangible form, or sold in high volume without restriction through telephone, mail order, or electronic transactions.[82] In addition, products qualifying for such treatment are those that have cryptographic functionality that cannot be easily modified by the user and has not been modified for the user, and do not require substantial support for installation and use.[83]

The EAR provides a non-exclusive list, subject to the above criteria, of "[e]xamples of eligible retail encryption products." The examples include:

- General purpose operating systems that do not qualify as mass-market;
- Non-programmable encryption chips, and chips that are constrained by design for retail products;
- Retail networking products such as low-end routers, firewalls, and virtual private networking (VPN) equipment designed for small office or home use;
- Desktop applications such as e-mail, browsers, games, word processing, database, financial applications or utilities, that do not qualify as mass-market;
- Programmable database management systems and associated application servers;
- Low-end servers and application-specific servers; and
- Short-range wireless components and software that do not quality as mass-market.[84]

---

[80] The definition of "retail" encryption items is contained in 15 C.F.R. § 740.17(b)(3)(i)(A). "Mass-market" encryption items are defined in Cryptography Note (Note 3) to Part II of Category 5 of the CCL. See further discussion in this subsection *infra*. The differences and similarities between "retail" and "mass-market" encryption products are explained by the BIS in its FAQ. See "U.S. Encryption Export Control Policy-Frequently Asked Questions (June 6, 2002), http://www.bxa.doc.gov/Encryption/EncFAQs6_17_02.html#10 (visited Feb. 3, 2003).

[81] See further discussion *infra*.

[82] 15 C.F.R. § 740.17(b)(3)(i)(A) (revised Sept. 23, 2002).

[83] 15 C.F.R. § 740.17(b)(3)(i)(B) (revised Sept. 23, 2002).

[84] 15 C.F.R. § 740.17(b)(3)(iii) (revised Sept. 23, 2002).

Certain other products will also be considered "retail," including encryption commodities and software (including key management products) with key lengths not exceeding specified lengths (e.g., not exceeding 64 bits for symmetric algorithms)[85] and encryption products and network-based applications that are equivalent in functionality to other "mass market" or retail encryption commodities.[86]

A "retail" encryption item controlled under ECCN 5A002 or 5D002 can be exported and reexported under License Exception ENC.[87] Such items may be exported and reexported to non-government end-users thirty days after the registration of a completed review request with BIS.[88] Certain of such items may remain subject to post-export reporting requirements.[89]

If the product is a "mass market" encryption commodity or software product,[90] it may be eligible to be exported and reexported under ECCN 5A992 or 5D992, following a thirty-day review period if the product employs a key length greater than 64 bits for the symmetric algorithm,[91] or following notification to the BIS if the key length is less than 64 bits.[92]

[iii]—"Open Cryptographic Interfaces" and Software Tools

Software or technology that cannot encrypt data may still be subject to the EAR if it can be combined with encryption to produce an encryption item.[93] Under the EAR, an "open cryptographic inter-

[85] 15 C.F.R. § 740.17(b)(3)(ii)(A) (revised Sept. 23, 2002).
[86] 15 C.F.R. § 740.17(b)(3)(ii)(B) (revised Sept. 23, 2002).
[87] 15 C.F.R. § 740.17(b)(3)(iii) (revised Sept. 23, 2002).
[88] 15 C.F.R. § 740.17(b)(3) (revised Sept. 23, 2002). Export or reexport to government end-users must await completion of BIS review. *Id.*
[89] 15 C.F.R. § 754.17(e) (revised Sept. 23, 2002).
[90] The term "mass-market" is defined in Cryptography Note (Note 3) to Part II of Category 5 of the CCL: "ECCNs 5A002 and 5D002 do not control items that 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: 1. Over-the-counter transactions; 2. Mail order transactions; 3. Electronic transactions; or 4. Telephone call transactions; b. The 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 the appropriate authority in the exporter's country in order to ascertain compliance with conditions described in paragraphs (a) through (c) of this note."
[91] *Id.*
[92] *Id.*

face"[94] is controlled as an encryption item.[95] Excluded from the definition are items that are designed to work with a fixed set of cryptographic algorithms that cannot be changed by the end-user and general application programming interfaces such as software development tools.[96] Open cryptographic interfaces may be eligible for the kinds of license exceptions applicable to other encryption items, such as License Exceptions ENC, which is concerned with encryption items generally and License Exception TSU, which is concerned with technology and software generally and includes an exception for certain "open source" software products.[97] If there is any doubt as to whether a product falls within the definition of an "open cryptographic interface," it is recommended that the product be submitted for a review and classification by the BIS.

[d]—General Prohibitions

A list of General Prohibitions exists for all items and services. These General Prohibitions apply to all exports, regardless of whether they fall under the CCL, the EAR99 designation, or a License Exception. If export of the item or service at issue falls under one of these General Prohibitions, then, unless a License Exception applies, a license application must be submitted before export may occur.[98]

---

[93] This policy is based on the government's concern that U.S. entities could circumvent the EAR by shipping unregulated technology (e.g., software without encryption) and then adding foreign-made encryption when the technology reached its offshore destination.

[94] Defined in 15 C.F.R. § 772.1: "A mechanism which is designed to allow a customer or other party to insert cryptographic functionality without the intervention, help or assistance of the manufacturer or its agents, e.g., manufacturer's signing of cryptographic code or proprietary interfaces. If the cryptographic interface implements a fixed set of cryptographic algorithms, key lengths or key exchange management systems, that cannot be changed, it will not be considered an 'open' cryptographic interface. All general application programming interfaces (e.g., those that accept either a cryptographic or non-cryptographic interface but do not themselves maintain any cryptographic functionality) will not be considered 'open' cryptographic interfaces."

[95] See 15 C.F.R. § 740.17(a), (b)(2), (d)(2) and (d)(3)(i), and *id.* Part 742, Supp. No. 6 (including instructions for completing review request form for an "open cryptographic interface."

[96] See 15 C.F.R. § 772.1 (definition of "open cryptographic interface").

[97] See § 8.05[5][g][i] and [ii] *infra*.

[98] These prohibitions include: (1) General Prohibition Four: Engaging in actions prohibited by a denial order; (2) General Prohibition Five: Export or reexport to prohibited end-uses or end-users; (3) General Prohibition Six: Export or reexport to embargoed destinations; (4) General Prohibition Seven: Support of proliferation activities; (5) General Prohibition Eight: In-transit shipments and items to be unladen from vessels or aircraft; (6) General Prohibition Nine: Violation of any order, terms, and conditions; (7) General Prohibition Ten: Proceeding with transactions with

In some circumstances, even though a License Exception would otherwise apply, the General Prohibitions may prohibit an intended export. For example, no License Exception exists that will allow an exporter to engage in actions prohibited by a denial order (General Prohibition Four). With respect to certain General Prohibitions, however, an export that would violate the General Prohibition could be made if the exporter meets the requirements of a given License Exception.[99] If these General Prohibitions do not apply, then any EAR99-classified item may be exported without a license. In such a situation, the item or service is exported "No License Required" (NLR).

[e]—The Country Chart

Located next to each specific ECCN on the CCL is a corresponding page number reference, which references the license requirements for that ECCN along with a detailed list of the items and/or services controlled under that ECCN and any License Exceptions for that ECCN. The license requirements set forth the reasons for the export control.[100] Next to each export control is a corresponding Country Chart identifier that cross-references a column on the Country Chart.[101] The Country Chart is a table that has the Country Chart

---

knowledge that a violation has occurred or is about to occur. A detailed description of these prohibitions is located at 15 C.F.R. § 736.2(b)(4)-(10) (revised June 19, 2000). General Prohibitions One, Two and Three are discussed at N. 102 *infra* and accompanying text.

[99] General Prohibitions One, Two, and Three may be superseded by any License Exception once the exporter has complied fully with the License Exception. 15 C.F.R. § 736.2(b) (revised June 19, 2000). General Prohibition Six may be superseded by License Exceptions authorized by Part 746 of the EAR. *Id.* General Prohibition 5 may be superseded by License Exceptions authorized in § 744.2(c) regarding nuclear end-users. *Id.*

[100] 15 C.F.R. § 742.15 (revised Sept. 23, 2002), setting forth the license requirements for encryption items, provides that such items are controlled because they "can be used to maintain the secrecy of information," and may be so used "by persons abroad to harm U.S. national security, foreign policy and law enforcement interests." This section also references the importance of protecting sensitive information in both the public and private sectors, and the requirements of the international Wassenaar Arrangement, which requires the U.S. to maintain control over the export and reexport of encryption items. See "The Wassenaar Arrangement—An Overview," at http://www.bxa.doc.gov/Wassenaar/Default.htm (visited Feb. 7, 2003). The reasons for other license requirements include: proliferation of chemical and biological weapons (CB), 15 C.F.R. § 742.2; nuclear nonproliferation (NP), *id.* § 742.3; national security (NS), *id.* § 742.4; missile technology (MT), *id.* § 742.5; regional stability (RS), *id.* § 742.6; crime control (CC), *id.* § 742.7, and anti-terrorism (AT), *id.* §§ 742.8-742.10; specially designed implements of torture, *id.* § 742.11; high performance computers (XP), *id.* § 742.12; communications interception devices, *id.* § 742.13; and significant items of aircraft technology (SI), *id.* § 742.14.

[101] The Country Chart is located at 15 C.F.R. Part 738, Supp. No. 1. The Country Chart does not apply to countries against which the United States has a general

identifiers set forth horizontally along the top of the chart, and a list of destination countries set forth vertically down the side of the chart. Using each applicable Country Chart identifier listed for a specific export control, if an "X" appears in the box of the Country Chart next to the destination country for the ECCN-classified item or service to be exported, a license will be required to export such item or service unless a License Exception is available.[102]

[f]—Applying for a License

A party requiring a license to export goods or services controlled under the EAC must file a license application with the Bureau of Industry and Security. Form BIS-748-P and related forms may be obtained by contacting the BIS.[103] To obtain a license, an applicant must complete the form and any required supporting documents and submit the application to the BIS for review. The applicant may apply for a license to export up to five items at the same time, using an Item Appendix form.[104] No filing fee is required for an export license.

In addition to the applicant's identifying information, the license application requires names and addresses of ultimate consignees (i.e., the party or parties to whom the item is shipped) and end-users. These may be the same entity; if not, a separate end-user must be listed on the license application. Several ultimate consignees or end-users may be listed on a supplemental form.[105] Export to certain country destinations may require the applicant to attach an Import or End-User Certificate, or a Statement by the Ultimate Consignee and Purchaser.[106] Import or End-User Certificates must be obtained from the ultimate consignees themselves or from the import authorities of the

---

embargo. Comprehensive controls currently apply to Cuba, Iran, Iraq, and Libya, to which different licensing requirements, licensing policies, and License Exceptions apply. 15 C.F.R. § 746.1(a) (revised Nov. 25, 2002). Rwanda is subject to supplemental controls. 15 C.F.R. § 746.1(b) (revised Nov. 25, 2002). Although subject to the EAR, items governed by short supply controls, such as crude oil and petroleum products, are subject to the license requirements and exceptions of 15 C.F.R. Part 754 (revised April 26, 2002). In addition, Angola is subject to special controls administered by the Office of Foreign Assets Control. *Id.* Part 746, Supp. No. 1 (revised Nov. 25, 2002).

[102] In such a situation, a license is required under General Prohibition One (Export and Reexport of Controlled Items to Listed Countries), General Prohibition Two (Parts and Components Reexports), and General Prohibition Three (Foreign-Produced Direct Product Reexports). *Id.* § 736.2(b)(1)-(3) (revised Aug. 29, 2002).

[103] See N. 70 *supra.* The BIS also has a system for electronic submission of applications. See http://www.bxa.doc.gov/fact sheets/facts5.htm.

[104] Form BIS-748P-A, Item Appendix.

[105] Form BIS-748P-B, End-User Appendix.

[106] 15 C.F.R. § 748.9 (revised June 6, 2002).

destination countries.[107] These documents provide additional information about how the recipient will use the item, including any intended reexport from the destination country.

The applicant must also describe the specific end-use to which the item will be applied. An applicant wishing to export cryptographic software may be required to submit technical specifications as well as a detailed description of the software's functionality. Additional information may be requested, such as how encrypted information can be retrieved for law-enforcement purposes.

[g]—License Exceptions

An item may be exported without a validated license otherwise required under General Prohibitions One, Two, or Three, if it falls within a License Exception set forth in the EAR,[108] and is not designated as EAR99 or NLR (No License Required). The License Exceptions can generally be broken down into two distinct categories: "list-based" and "transaction-based." The list-based exceptions are those whose applicability is determined primarily by the specifications and parameters of the applicable ECCN, while the transaction-based exceptions are those whose applicability is determined primarily by the specifics of the transaction, such as the end-use and the identity of the end-user.[109] The list-based License Exceptions are available to an exporter only to the extent that they are allowed on the Commerce Control List.[110] For example, encryption software, designated as 5D002 on the CCL, has no such list-based License Exceptions.[111]

In contrast, the transaction-based License Exceptions[112] are specific to the item being exported and to factors concerning that particular export. Each such License Exception has different eligibility

---

[107] 15 C.F.R. § 748.10(c) (revised June 6, 2002); 15 C.F.R. Part 748, Supp. No. 4 (listing foreign authorities from whom the certificates may be obtained) (revised June 6, 2002).

[108] 15 C.F.R. Part 740, (revised June 19, 2000). Exports or reexports subject to General Prohibitions Four, Seven, Eight, Nine, or Ten have no License Exceptions in Part 740, while the availability of License Exceptions for General Prohibition Six is determined by 15 C.F.R. Part 746, and for General Prohibition Five, by 15 C.F.R. Part 744. 15 C.F.R. § 740.1(a) (revised Sept. 28, 2002); 15 C.F.R. § 736.2(b) (revised Aug. 29, 2002). With respect to General Prohibition Eight (intransit shipments), see 15 C.F.R. § 736.2(8), prohibiting intransit shipment to specified countries unless a license or License Exception allows direct shipment to such country, or unless no license is required for that item.

[109] See http://www.bxa.doc.gov/factsheets/ExportGuidance.html (visited Feb. 3, 2003).

[110] 15 C.F.R. § 732.4(b)(3)(iii) (revised June 6, 2002).

[111] See 15 C.F.R. Part 774, Supp. No. 1(revised Jan. 19, 2000).

[112] The transaction-based License Exceptions include: (1) key management infrastructure (KMI), 15 C.F.R. 740.8; (2) temporary imports, exports, and reexports

requirements, but the requirements for these License Exceptions are generally based on factors such as: the item being exported or reexported, the country of ultimate destination, the end-use and the end-user, and any other special conditions required by a given License Exception. As a result, each transaction-based License Exception should be reviewed to determine whether the specific export or reexport being undertaken falls within such a License Exception. Generally, if a transaction-based License Exception does not specifically exclude encryption items or services, then that License Exception may be used, provided that the export action itself is an excluded transaction. For example, the GOV License Exception may be used to export encryption items or services to members of the United States Armed Forces or to civilian personnel of the United States government for their personal use,[113] but the GOV License Exception may not be used to export encryption items or services to diplomatic or consular missions of certain governments for their official use.[114]

[i]—License Exception KMI (Key Management Infrastructure)

Transaction-based License Exception KMI was specifically created to address issues relating to encryption items. Encryption equipment, assemblies and components of encryption software may be made eligible for License Exception KMI under a "key recovery" program.[115] The government would be given access to these keys under certain prescribed conditions.[116] To be eligible, exporters must submit a classification request to the BIS, which will perform a one-time review.[117]

[ii]—License Exception ENC (Encryption Commodities and Software)

Encryption commodities, software, and components may be

(TMP), *id.* § 740.9; (3) servicing and replacement of parts and equipment (RPL), *id.* § 740.10; (4) governments, international organizations and international inspections under the Chemical Weapons Convention (GOV), *id.* § 740.11; (5) gift parcels and humanitarian donations (GFT), *id.* § 740.12; (6) technology and software—unrestricted (TSU), *id.* § 740.13; (7) baggage (BAG), *id.* § 740.14; and (8) aircraft and vessels (AVS), *id.* § 740.15.

[113] 15 C.F.R. § 740.11(b)(2)(i) (revised Sept. 23, 2002).

[114] 15 C.F.R. § 740.11(b)(2)(iv) (revised Sept. 23, 2002).

[115] The requirements and procedures for qualifying for the key escrow or key recovery program are set forth at 15 C.F.R. Part 742, Supp. No. 4 (revised Sept. 23, 2002).

[116] Such keys must be made available to "government officials under proper legal authority and without the cooperation or knowledge of the user." 15 C.F.R. Part 742, Supp. 4(2) (revised Sept. 23, 2002).

[117] 15 C.F.R. § 740.8 (revised Sept. 23, 2002). The exception covers encryption software and commodities "of any key length controlled under ECCNs 5A002 and 5D002." *Id.* § 740.8(b)(1).

eligible for export or reexport under License Exception ENC.[118] Depending upon the circumstances of the transaction and the nature of the items involved, License Exception ENC may permit export and reexport without review by BIS, or upon the expiration of thirty days after registration of a completed review request.[119] The export of products falling under License Exception ENC is, however, still subject to the EAR's other general prohibitions.[120] License Exception ENC allows immediate export and reexport of most encryption items controlled under ECCNs 5D002 and 5E002, to both government and non-government users, to certain countries such as Australia, Austria, Belgium, the Czech Republic, and others listed in Supplement 3 to Part 740, following a one-time review by the BIS.[121]

License Exception ENC allows United States companies to export encryption items of any key length, including source code and technology for internal company use, to their international subsidiaries *without* a one-time review by the BIS. The encryption items may be used by the international subsidiary to develop new products, which it may then, without the BIS's approval, export back to the United States or to other international subsidiaries of the same parent.[122] United States companies may also transfer encryption technology to their foreign employees[123] in the United States for internal company use, including development of new products. All items so developed

---

[118] 15 C.F.R. § 740.17, "Encryption Commodities and Software." License Exception ENC first appeared in the Interim Rule of December 31, 1998. On September 16, 1999, the administration announced its intention of expanding the scope of License Exception ENC. This expanded exception was codified in the January 14, 2000 Interim Final Rule, 65 Fed. Reg. 2499 (Jan. 14, 2000). License Exception ENC has been amended several times subsequently, see 65 Fed. Regs. 62600, 62605 (Oct. 19, 2000) and 67 Fed. Regs. 38855, 38862 (June 6, 2002). The most recent changes, part of amendments to the EAR that implemented the changes made to the Wassenaar Arrangement List of dual-use items, made substantive changes as well as changes for clarification of the exception.

[119] The term "registration" is defined in 15 C.F.R. § 750.4(a)(2).

[120] See, e.g., 15 C.F.R. § 740.17 (stating that exports and reexports under License Exception ENC "remain subject to "EI" controls). This also includes prohibitions on exports to embargoed countries and to "denied persons." See § 8.05[5](d) *supra;* see also, the relevant rules of the Department of Commerce and the State Department for updated information.

[121] 15 C.F.R. § 740.17(a) (revised Sept. 23, 2002) (excepting cryptanalytic items). The countries listed in Supplement No. 3 to Part 740 are Austria, Australia, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, Netherlands, New Zealand, Norway, Poland, Portugal, Spain, Sweden, Switzerland, and the United Kingdom.

[122] 15 C.F.R. § 740.17(b)(1) (Sept. 23, 2002).

[123] The company may not, however, transfer the encryption technology to its employees who are nationals of countries listed in Country Group E:I of Part 740, Supp. No. 1, i.e., Cuba, Iran, Iraq, Libya, North Korea, Sudan or Syria. *Id.*

(by an international subsidiary or a foreign employee in the United States) with encryption commodities are, however, subject to the EAR and must be reviewed and classified before being sold or retransferred outside the United States company.[124]

In countries not listed on Supplement 3 to Part 740, License Exception ENC also allows the export and reexport to any non-government end-user of any encryption commodity, software, and component thirty days after registration of a completed review request by the BIS under ECCNs 5A002 and 5D002.[125] This includes network infrastructure products, proprietary encryption code (i.e., encryption code that is not considered "publicly available" under License Exception TSU), general purpose toolkits,[126] cryptanalytic items, and encryption items not otherwise authorized for export as mass-market or retail.[127] Such products may be exported and reexported to government end-users in countries not listed in Supplement No. 3 to Part 740 only under a license.[128] Retail encryption commodities, software, and components, on the other hand, may be exported and reexported to non-government end-users under License Exception ENC thirty days after the registration of a completed review request with the BIS, and to government users after the completion of BIS review and authorization.[129]

[iii]—License Exception TSU (Technology and Software—Unrestricted)

The License Exception for Technology and Software—Unrestricted (TSU) authorizes the export and reexport of certain operation technology and software, sales technology and software, software updates (bug fixes), mass-market software subject to the General Software Note, and unrestricted encryption source code.[130] Open-source encryption software[131] is released from export controls,

---

[124] See *id.*

[125] 15 C.F.R. § 740.17(b)(2) (revised Sept. 23, 2002) (excepting items that provide an open cryptographic interface).

[126] Application-specific toolkits are covered under "components" in Part 772 of the EAR. 15 C.F.R. § 740.17.

[127] *Id.* § 740.17(b)(3)(ii).

[128] 15 C.F.R. § 740.17(b)(2) (revised Sept. 23, 2002).

[129] 15 C.F.R. § 740.17(b)(3) (revised Sept. 23, 2002). See § 8.05[5][c][ii] *supra* (discussing retail encryption commodities and software).

[130] 15 C.F.R. § 740.13 (revised Sept. 23, 2002) (specifying categories, uses, and destinations to which License Exception TSU apply). This discussion focuses, however, on the encryption software regulations.

[131] I.e., "source code controlled under ECCN 5D002 that would be considered publicly available under § 734.3(b)(3) of the EAR, and corresponding object code resulting from the compiling of such source code." 15 C.F.R. § 740.13(e).

without BIS review. The exporter must give the BIS notice by the time of export, including either the Web site or other Internet location where the source code will be posted, or a copy of the source code to be exported.[132]

Although exporters of proprietary source code or object code may be required to take precautions to reduce the risk that software available on the Internet will be downloaded to enemy countries,[133] exporters of open source software who have given the BIS appropriate notice are exempt from the reverse-DNS lookup requirement. "Knowingly" exporting open source software to enemy countries (Cuba, Iran, Iraq, Libya, North Korea, Sudan or Syria) is forbidden, but merely operating a Web site from which the code may be downloaded does not in itself constitute "knowledge."[134]

All License Exceptions are subject to certain general restrictions. The License Exceptions may not be used if: (1) the authorization to use an applicable License Exception has been suspended or revoked or the intended export does not have a License Exception; (2) a Denial Order prohibits the export;[135] (3) the exporter knows that the item is going to be reexported, that the reexport is subject to a General Prohibition to which there is no License Exception, and that the BIS has not authorized such reexport; and (4) the item or service is to be exported to certain end-users or for certain end-uses provided for and prohibited by the EAR.[136] In addition, the BIS has the authority to revoke, suspend, or revise any License Exception without notice.[137] If none of the above restrictions applies, any applicable License Exception may be used so long as its eligibility requirements are met.[138]

---

[132] 15 C.F.R. § 740. 13(e)(5) (revised Sept. 23, 2002).

[133] These precautions include implementing reverse-DNS lookup (a means of analyzing the address of the computer making the request to download the software), providing notice that the software is subject to the EAR, and obtaining the user's consent to EAR restrictions applicable to the software, usually in a form similar to that of a clickwrap license. See: 15 C.F.R. § 734.2(b)(9)(iii); § 8.05[5][b] *supra*.

[134] 15 C.F.R. § 740.13(e)(6) (revised Sept. 23, 2002). This provision, of course, does not prevent the BIS from determining, based on other evidence, that the exporter had "knowledge" of an export to a restricted destination. It is currently unknown what the consequences would be to an exporter that allowed a download of open source to an enemy country.

[135] Denial Orders prohibiting many actions may be issued by the BIS, including export privileges of individuals who violate the EAR. See 15 C.F.R. Part 764 (specifying standard terms of orders denying export privileges) (revised Aug. 29, 2002).

[136] See 15 C.F.R. § 740.2(a) for such provisions and prohibitions (revised Sept. 23, 2002). Some of these restrictions are discussed in greater detail at 15 C.F.R. Part 744.

[137] 15 C.F.R. § 740.2(b) (revised Sept. 23, 2002).

[138] The applicability of all License Exceptions to General Prohibition Five is described at 15 C.F.R. Part 744 ("Control Policy: End-User and End-User Based")

[h]—Reporting Requirements

Exporters of encryption may be required to report the exported product's classification, the number of units shipped, and the destination of the shipment. These requirements do not apply to exports to United States subsidiaries for internal use, retail products exported to individual consumers, software exported by free or anonymous download, encryption items with less than 64-bit symmetric key length, certain short-range wireless encryption items, retail operating systems and desktop applications for single-CPU computers, laptops, and hand-held devices, certain Internet appliance and LAN cards, foreign products developed by bundling or compiling source code, or exports from United States financial institutions to affiliates, customers, or contractors for "financial-specific" purposes.[139] The BIS may request additional information, which exporters are obligated to provide under the EAR. Exporters should review the EAR to determine which, if any, reporting requirements apply.

[i]—Violations of the EAR

The EAR prohibits certain acts and punishes such acts with several types of sanctions. Violations include:

(1) Engaging in conduct that violates, or not engaging in conduct required by, the EAR, or any authorization, order, or license issued thereunder;

(2) Aiding or abetting in the violation of the EAR or any authorization, order, or license issued thereunder;

(3) Soliciting, attempting or conspiring with someone to violate the EAR or any authorization, order, or license issued thereunder;

(4) Acting with the knowledge of a violation, possession of a restricted item with the intent to export illegally, or misrepresentation or concealment in connection with the application process and any government investigation.[140]

---

and the applicable License Exceptions to General Prohibition Six are located in 15 C.F.R. Part 746 ("Embargoes and Other Special Controls"). Those items controlled as short supply items have License Exceptions located in 15 C.F.R. Part 754. If multiple License Exceptions apply to a given export or reexport, only one of those License Exceptions need be used as a basis to avoid filing.

[139] 15 C.F.R. § 740.17(e)(4) (revised Sept. 23, 2002).

[140] A complete list of violations can be found at 15 C.F.R. § 764.2 (revised Aug. 29, 2002).

These violations could subject the exporter to sanctions.[141] Civil administrative sanctions include civil penalties that may be as high as $10,000, or as high as $100,000 if national security controls are violated, and may also include the denial of export privileges to the named person or a restriction on the named person's access to the items subject to the EAR.[142] "Criminal sanctions" for general violations include fines of up to five times the value of the exports involved or $50,000, whichever is greater, and/or five years in prison.[143] Willful violations are punishable by fines of up to five times the value of the exports involved or $1,000,000, whichever is greater, when the violation is committed by entities, and fines up to $250,000 and/or prison terms of up to ten years when the violation is committed by an individual.[144] Criminal sanctions provided for under conspiracy,[145] false statements,[146] mail and wire fraud,[147] and money laundering[148] laws may also be imposed.[149] Other sanctions include statutory sanctions on imports and procurement, for violations related to weapons proliferation, and seizure and forfeiture of the items and of the vessels, vehicles, and aircraft carrying those items, exported in violation of the EAA or EAR, or orders, licenses, or authorization issued thereunder.[150] With certain limitations, the EAR also provides a mechanism by which an exporter may voluntarily disclose its belief that it is violating the EAR or any authorization, order, or license issued thereunder.[151] Such disclosure is a mitigating factor in the BIS's determination in assessing administrative sanctions, if any.

(Text continued on page 8-67)

---

[141] See 15 C.F.R. § 764.3 (revised Aug. 29, 2002) for a discussion of all applicable sanctions.

[142] *Id.* § 764.3(a)(2) (revised Aug. 29, 2002). The Denied Persons List sets forth those persons denied export privileges by the BIS and can be found at *id.* Part 764, Supp. No. 2.

[143] *Id.* § 764.3(b)(1) (revised Aug. 29, 2002).

[144] *Id.* § 764.3(b)(2)(i) (revised Aug. 29, 2002). An individual licensed to export or reexport to a controlled country who knows the end-use is a military or intelligence-gathering one, and who willfully fails to report such use, is subject to the same fines or a maximum of five years in prison. *Id.* § 764.3(b)(2)(ii).

[145] 18 U.S.C. § 371.

[146] 18 U.S.C. § 1001.

[147] 18 U.S.C. §§ 1341, 1343, and 1346.

[148] 18 U.S.C. §§ 1956 and 1957.

[149] See 15 C.F.R. § 764.3(b)(3).

[150] 15 C.F.R. § 764.3(c) (revised Aug. 29, 2002).

[151] *Id.* § 764.5 (revised Aug. 29, 2002).