C

Appendix C: U.S. Export Controls on Cryptography

The United States has two regulatory regimes for exports, depending on whether the item to be exported is military in nature, or is "dual-use," having both civilian and military uses. These regimes are administered by the State Department and the Commerce Department, respectively. Both regimes provide export controls on selected goods or technologies for reasons of national security or foreign policy. Licenses are required to export products, services, or scientific and technical data[1] originating in the United States, or to re-export these from another country.

Licensing requirements vary according to the nature of the item to be exported, the end use, the end user, and, in some cases, the intended destination. For many items that are under Commerce jurisdiction, no specific approval is required and a "general license" applies (e.g., when the item in question is not military or dual-use and/or is widely available from foreign sources). In other cases, an export license must be applied for from either the State Department or the Commerce Department, depending on the nature of the item. In general, the State Department's licensing requirements are more stringent and broader in scope.[2]

[1] Both the Export Administration Act (50 U.S.C. App. 2401-2420) and the Arms Export Control Act (22 U.S.C. 2751-2794) provide authority to control the dissemination to foreign nationals (export) of scientific and technical data related to items requiring export licenses under the regulations implementing these acts. "Scientific and technical data" can include plans, design specifications, or other information that describes how to produce an item. See U.S. Congress, Office of Technology Assessment, *Information Security and Privacy in Network Environments,* OTA-TCT-606 (Washington, DC; U.S. Government Printing Office, September 1994), pp. 150-160.

Other statutory authorities for national security controls on scientific and technical data are found in the Restricted Data or "born classified" provisions of the Atomic Energy Act of 1946 (60 Stat. 755) and the Atomic Energy Act of 1954 (68 Stat. 919, 42 U.S.C. 2011-2296), and in the Invention Secrecy Act of 1951 (35 U.S.C. 181-188), which allows for patent secrecy orders and withholding of patents on national security grounds. NSA has obtained patent secrecy orders on patent applications for cryptographic equipment and algorithms under authority of the Invention Secrecy Act.

[2] For another comparison of the two export-control regimes, see U.S. General Accounting Office, *Export Controls: Issues in Removing Militarily Sensitive Items from the Munitions List,* GAO/NSIAD-93-67 (Washington, DC: U.S. Government Printing Office, March 1993), esp. pp. 10-13.

The material in this appendix is taken from pages 150-160 of the 1994 OTA report, updated where appropriate. Licensing terms differ between the agencies, as do time frames and procedures for licensing review, revocation, and appeal.

STATE DEPARTMENT EXPORT CONTROLS ON CRYPTOGRAPHY

The Arms Export Control Act and International Traffic in Arms Regulations (ITAR),[3] administered by the State Department, control export of items (including hardware, software, and technical data) that are "inherently military in character" and, therefore, placed on the Munitions List.[4] Unless otherwise indicated, items on the Munitions List are controlled to all destinations, meaning that "validated" licenses—requiring case-by-case review—are required for any exports (except to Canada, in some cases). The Munitions List is established by the State Department, in concurrence with the Defense Department; the State Department's Office of Defense Trade Controls administers the ITAR and issues licenses for approved exports. The Defense Department provides technical advice to the State Department when there are questions concerning license applications or commodity jurisdiction (i.e., whether State or Commerce regulations apply—see below).

With certain exceptions, cryptography falls in "Category XIII—Auxiliary Military Equipment" of the Munitions List. Category XIII(b) covers "Information Security Systems and equipment, cryptographic devices, software and components specifically designed or modified therefore," generally including:

1. cryptographic and key-management systems and associated equipment, subcomponents, and software capable of maintaining information or information-system secrecy/confidentiality;
2. cryptographic and key-management systems and associated equipment, subcomponents, and software capable of generating spreading or hopping codes for spread-spectrum systems or equipment;
3. cryptanalytic systems and associated equipment, subcomponents, and software;
4. systems, equipment, subcomponents and software capable of providing multilevel security that exceeds class B2 of the National Security Agency's (NSA's) Trusted Computer System Evaluation Criteria, as well as software used for certification;
5. ancillary equipment specifically designed or modified for these functions; and
6. technical data and defense services related to the above.[5]

Several exceptions apply to item XIII(b)(1) above. These include the following subcategories of cryptographic hardware and software:

a. those used to decrypt copy-protected software, provided that the decryption functions are not user-accessible;
b. those used only in banking or money transactions (e.g., in ATM machines and point-of-sale terminals, or for encrypting interbanking transactions);
c. those that use analog (not digital) techniques for cryptographic processing in certain applications, including facsimile equipment, restricted-audience broadcast equipment, and civil television equipment;
d. those used in personalized smart cards when the cryptography is of a type restricted for use only in applications exempted from Munitions List controls (e.g., in banking applications);

[3] 22 C.F.R. 120-130.

[4] See Supplement 2 to Part 770 of the Export Administration Regulations. The Munitions List has 21 categories of items and related technologies, such as artillery and projectiles (Category II) or toxicological and radiological agents and equipment (Category XIV). Category XIII(b) consists of "Information Security Systems and equipment, cryptographic devices, software, and components specifically modified therefore."

[5] Ibid. See Category XIII(b)((1)-(5)) and XIII(k). For a review of controversy during the 1970s and early 1980s concerning control of cryptographic publication, see F. Weingarten, "Controlling Cryptographic Publication," *Computers & Security*, vol. 2, 1983, pp. 41-48.

e. those limited to access-control functions (e.g., for ATM machines, point-of-sale terminals, etc.) in order to protect passwords, personal identification numbers, and the like provided that they do not provide for encryption of other files or text;
f. those limited to data authentication (e.g., calculating a message authentication code) but not allowing general file encryption;
g. those limited to receiving radio broadcast, pay television, or other consumer-type restricted audience broadcasts, where digital decryption is limited to the video, audio, or management functions and there are no digital encryption capabilities; and
h. those for software designed or modified to protect against malicious computer damage from viruses, and so forth.[6]

Cryptographic hardware and software in these subcategories are excluded from the ITAR regime and fall under Commerce's jurisdiction. Note, however, that these exclusions do not include hardware-based products for encrypting data or other files before transmission or storage, or user-accessible, digital encryption software for ensuring email confidentiality or read-protecting stored data or text files. These remain under State Department control.

In September 1994, the State Department announced an amendment to the regulations implementing section 38 of the Arms Export Control Act.[7] The new rule implements one of the reforms applicable to encryption products that were announced on February 4, 1994, by the State Department.[8] It established a new licensing procedure in the ITAR to permit U.S. encryption manufacturers to make multiple shipments of items covered by Category XIII(b)(1) of the Munitions List (see above) directly to end users in an approved country, without obtaining individual licenses. Previously, only those exports covered by a distribution arrangement could be shipped without an individual license; the new procedure permits direct distribution from manufacturers without foreign distributors. The procedures are similar to existing distribution agreement procedures; exporters submit a proposed arrangement specifying items to be shipped, proposed end users and uses, and destination countries. Upon approval, exporters can ship the specified products directly to the end users in the approved countries, with a single license.[9] Among the other reforms announced in February 1994 but awaiting implementation are special licensing procedures that would permit export of key-escrow encryption products to "most" end users.[10]

COMMERCE DEPARTMENT EXPORT CONTROLS ON CRYPTOGRAPHY

The Export Administration Act (EAA)[11] and Export Administration Regulations (EAR),[12] administered by the Commerce Department, are designed to control exports of "sensitive" or dual-use items, including software and scientific and technical data. Some items on the Commerce Control List (CCL) are controlled for national security purposes, to prevent them from reaching "proscribed" countries (usually in the former So-

[6] Munitions List, ibid. See XIII(b) (1) (i)-(ix).

[7] Department of State, Bureau of Political-Military Affairs, 22 CFR parts 123 and 124, *Federal Register*, vol. 59, No. 170, Sept. 2, 1994, pp. 45621-45623.

[8] Martha Harris, Deputy Assistant Secretary for Political-Military Affairs, U.S. Department of State, "Encryption—Export Control Reform," statement, Feb. 4, 1994.

[9] *Federal Register*, op. cit., footnote 7, p. 45621.

[10] Martha Harris, op. cit., footnote 8.

[11] At this writing, the export administration legislation is to be reauthorized.

[12] 22 U.S.C. 2751-2794.

viet bloc); others are controlled for various foreign policy objectives.[13]

The Bureau of Export Administration administers controls on dual-use items. The Bureau of Export Administration's Office of Strategic Trade and Foreign Policy Controls [14] is responsible for making licensing determinations, coordinating with other responsible agencies as necessary, and maintaining the Commerce Control List for cryptographic products.[15]

Cryptography falls under Section II ("Information Security") of the CCL.[16] This category includes information-security "equipment, assemblies and components" that:

1. are designed or modified to use digital cryptography for information security;
2. are designed or modified to use cryptanalytic functions;
3. are designed or modified to use analog cryptography, except for some low-speed, fixed band scrambling or frequency inversion, or in facsimile equipment, restricted audience broadcast equipment or civil television equipment (see item c above);
4. are designed to suppress compromising emanations of information-bearing signals, except for suppression of emanations for health or safety reasons;
5. are designed or modified to use cryptography to generate the spreading code for spread-spectrum systems or the hopping code for frequency agility systems; or
6. are designed or modified to exceed class B2 of the Trusted Computer System Evaluation Criteria (see item 4 in the State Department list above); plus those that
7. are communications cable systems with intrusion-detection capabilities.

Equipment for the test, inspection, and production (including evaluation and validation equipment) of equipment or functions in this category are included, as are related software and technology.

OVERLAP BETWEEN CONTROL REGIMES

The "overlap" between the State Department and Commerce Department export-control regimes is particularly complex for cryptography (note the overlap between the Munitions List items and the CCL items shown above, even with the exceptions). Basically, the Commerce Department licenses only those Section II items that are either excepted from State Department control, are not controlled, or are eligible for licensing under an advisory note, plus anti virus software (see item h in the section on State Department controls above).[17] The cryptographic items exempted from control under advisory note 1 are: personalized smart cards as described in item d above; equipment for fixed data compression or coding techniques, or for use in applications described in item g above; portable, commercial civil cellular phones containing encryption, when accompany-

[13] See GAO, op. cit., footnote 2, pp. 10-12.

[14] The functions of the Office of Export Licensing and the Office of Technology and Policy Analysis were merged and shifted after a reorganization of the Bureau of Export Administration in late 1994-early 1995. (Maurice Cook, Bureau of Export Administration, Economic Analysis Division, personal communication, Mar. 17, 1995.)

[15] Joseph Young, Office of Strategic Trade and Foreign Policy Controls, Bureau of Export Administration, personal communication, Mar. 23, 1995.

[16] See Supplement 1 to Part 799.1 of the Export Administration Regulations, sections A (equipment, assemblies and components), B (test, inspection, and production equipment), D (software), and E (technology).

[17] Ibid., p. CCL123 (notes). The advisory notes specify items that can be licensed by Commerce under one or more administrative exceptions.

ing their users; and software as described in item a above.[18] Other items, such as cellular phone systems for which message traffic encryption is not possible or items for civilian use in banking, access control, and authentication as described under items b), e), or f) above, are covered by advisory notes 3 through 5. These advisory notes state that these items are likely to be licensed by Commerce, as administrative exceptions, for export to acceptable end users.[19]

At present, software and hardware for robust, user-controlled encryption remains on the Munitions List under State Department control, unless State grants jurisdiction to Commerce.[20] This has become increasingly controversial, especially for the information technology and software industries. According to the U.S. General Accounting Office's (GAO's) 1993 report:

> NSA performs the technical review that determines, for national security reasons, (1) if a product with encryption capabilities is a munitions item or a Commerce List item and (2) which munitions items with encryption capabilities may be exported. The Department of State examines the NSA determination for consistency with prior NSA determinations and may add export restrictions for foreign policy reasons—e.g., all exports to certain countries may be banned for a time period.
>
> . . . [T]he detailed criteria for these decisions are generally classified. However, vendors exporting these items can learn some of the general criteria through prior export approvals or denials they have received. NSA representatives also advise companies regarding whether products they are planning would likely be munitions items and whether they would be exportable, according to State Department representatives.[21]

At the end of COCOM in 1994, the Clinton Administration liberalized the policy for some exports of computer and telecommunications products to Russia, Eastern Europe, and China. However, controls were maintained on cryptography because:

> The President has determined that vital U.S. national security and law enforcement interests compel maintaining appropriate control of encryption.[22]

In 1992, there had been limited relaxation of export controls for mass-marketed software with encryption capabilities. NSA and the State Department relaxed and streamlined export controls for mass-market software with moderate encryption capabilities, but not including software implementing the Data Encryption Standard (DES) or computer hardware containing encryption algorithms.[23] Also, since July 1992, there has been expedited review of software using one of two algorithms developed by RSA Data Security, Inc. These algorithms, called RC2 and RC4, are said to be significantly stronger than those previously allowed for export, but are limited to a 40-bit key length and are said to be weaker than the "DES-strength" programs that can be marketed in the United States and that are available overseas.

U.S. software producers still face the ITAR restrictions (with the new, expedited-distribution rule noted above) for exports of software with strong encryption.[24] Software or hardware products using the DES for message encryption (as opposed to message authentication) are on the Munitions List and are generally nonexportable to foreign commercial users, except foreign subsidiaries of U.S. firms and some financial institutions

[18] Ibid., pp. CCL123-126. Software required for or providing these functions is also excepted.

[19] Ibid., Advisory Notes 1-5.

[20] GAO, op. cit., footnote 2, pp. 24-28.

[21] Ibid., p. 25.

[22] Martha Harris, op. cit., footnote 8.

[23] Ibid.

[24] "Strong" encryption in this context refers to systems on a par with the DES or with the RSA system with a 1,024-bit modulus.

(for use in electronic funds transfers). Products that use the DES and other algorithms for purposes other than message encryption (e.g., for authentication) can be exported on the Commerce Control List, however.[25]

In the 103d Congress, legislation intended to streamline controls and ease restrictions on mass-market computer software, hardware, and technology, including certain encryption software, had been introduced. No export legislation was enacted, however, and the last reported version of the House legislation did not include these provisions.[26] In the 104th Congress, omnibus export administration legislation for 1995 has been introduced in the House (H.R. 361). At this writing, it does not have special provisions for cryptography.

[25] GAO, op. cit., footnote 2, p. 26. For discussion of industry and government views, OTA, op. cit., footnote 1, pp. 154-160.

[26] See U.S. Congress, House of Representatives, *Omnibus Export Administration Act of 1994,* H. Rept. 103-531, 103d Cong., 2d sess., Parts 1 (Committee on Foreign Affairs, May 25, 1994), 2 (Permanent Select Committee on Intelligence, June 16, 1994), 3 (Committee on Ways and Means, June 7, 1994), and 4 (Committee on Armed Services, June 17, 1994) (Washington, DC, U.S. Government Printing Office, 1994); and H.R. 4663, "Omnibus Export Administration Act of 1994," June 28, 1994.