Return to Table of Contents

CHAPTER 10

Encryption
(Section 742.15)

Export Control Program Description and Licensing Policy

On December 30, 1996, BXA issued an interim rule in the *Federal Register* (61 FR 68572) that exercised jurisdiction over dual-use encryption products. The rule imposed national security and foreign policy controls on certain cryptographic items, including commercial encryption "software" and "hardware," that were on the United States Munitions List (USML). This action was taken consistent with Executive Order (E.O.) 13026 and pursuant to the Presidential Memorandum, both of which were issued by President Clinton on November 15, 1996. The Memorandum and E.O. 13026 directed that all encryption items controlled on the USML, with the exception of those specifically designed, developed, configured, adapted, or modified for military applications (including command, control, and intelligence applications), be transferred to the Commerce Control List (CCL). The items specifically designed for military applications remain on the USML and continue to be controlled by the Office of Defense Trade Controls at the Department of State.

In the CCL the acronym "EI" (Encryption Items) designates cryptographic items for which the highest level of national security-based controls are applied under the Export Administration Regulations (EAR). Accordingly, such items are subject to certain unique restrictions under the EAR. For instance, exporters must notify BXA, or else provide a copy of the source code, prior to making EI-controlled encryption software freely and publicly available (e.g., by posting to the Internet) under license exception Technology and Software Unrestricted (TSU). In addition, EI controlled parts, components, software, and technology are not eligible for *de minimis* treatment when incorporated into foreign products, absent specific authorization by BXA.

U.S. encryption policy rests on three tenets: a review of encryption products in advance of sale, a streamlined post-export reporting system, and a license process that preserves the U.S. Government's ability to review the sale of strong encryption to foreign governments, military organizations, and nations of concern. Just as the market for information security products has grown and changed, this policy continues to evolve consistent with national interest in areas such as electronic commerce, national security, and support to law enforcement. The Administration's encryption policy makes it easier for

Americans to use stronger encryption products to protect their privacy, intellectual property, and other valuable information.

Since the publication of the interim rule in 1996, export controls on encryption have evolved, with the most recent announcement updating controls being made on October 19, 2000. Key features of the current regulations are described in the following paragraphs.

U.S. companies can export encryption products and technology under a license exception to any end-user in the 15 nations of the European Union as well as Australia, Norway, Czech Republic, Hungary, Poland, Japan, New Zealand, and Switzerland immediately upon notifying BXA of intent to export.

Any encryption commodity or software can be exported under a license exception, after a technical review, to any non-government end-user worldwide, except for sanctioned or embargoed destinations, or denied persons. To ensure streamlined exports to non-government end-users, companies may export products under this provision 30 days after submitting the products for technical review.

Any encryption item, including encryption technology and source code, except encryption technology to nationals of Cuba, Iran, Iraq, Libya, North Korea, Sudan, or Syria, may be released to foreign nationals working for U.S. companies in the United States for internal company use without review by BXA. Exports or transfers of encryption technology to nationals of designated terrorist-supporting countries require a license.

A category of products called "retail encryption commodities and software" may be exported after technical review to any end-user, including government end-users, under a license exception. Retail encryption commodities and software are generally available to the public, are easy to install, and implement cryptography that cannot be easily changed, modified, or customized by the customer. This category includes financial-related products intended for use by banks, financial institutions, and other approved sectors. Certain restrictions apply to telecommunications and Internet service providers, and network infrastructure products such as high-end routers and switches may not be exported under these retail provisions.

Products that incorporate components providing cryptographic functionality limited to short-range wireless technology can be exported under a license exception to any end-user. These items include consumer products such as audio devices, cameras, video recorders, computer accessories, hand held devices, mobile phones, and household appliances. These products do not require review by BXA and are exempt from post-export reporting requirements.

To facilitate the development of next-generation products and to allow more market flexibility, products that enable U.S. and non-U.S. source products to operate together may also be immediately exported. Licenses are only required for "cryptanalytic items," a specialized class of tools not normally used in commercial environments, and "open cryptographic interface" products which provide an "open door" for the insertion of foreign or customized cryptography.

Post-export reporting under the encryption license exception ensures compliance with U.S. regulations and has allowed the Administration to reduce licensing requirements for non-embargoed destinations. Reporting is no longer required for products exported by U.S.-owned overseas subsidiaries, retail operating systems, and desktop applications (such as e-mail programs and browsers) designed for, bundled with, or pre-loaded on single central processing unit devices such as personal computers, laptops, or hand held devices.

Exporters can self-classify unilaterally controlled encryption products that are subject to foreign policy controls only (i.e., items classified under ECCNs 5A992, 5D992, and 5E992) upon notification to BXA. Validated licenses are required on exports by U.S. persons to designated terrorist-supporting countries (Cuba, Iran, Iraq, Libya, North Korea, Sudan, or Syria), their nationals, and other sanctioned entities.

Analysis of Control as Required by Section 6(f) of the Act

A. The Purpose of the Control

Encryption export controls are in place to protect U.S. national security, foreign policy, and law enforcement interests, particularly as they relate to the safety of U.S. citizens at home and abroad. Encryption can be used to conceal the communications of, for example, terrorists, drug smugglers, and other individuals intent on taking actions harmful to U.S. facilities, personnel, or security interests. Use of cryptographic products by criminals and terrorists makes it more difficult for law enforcement agencies to uncover and prevent hostile acts before they occur. Cryptographic products and software also have military and intelligence applications that, in the hands of hostile nations, could pose a threat to U.S. national security. These controls are consistent with E.O. 13026 of November 15, 1996, and the Presidential Memorandum of the same date.[1]

B. Considerations and/or Determinations of the Secretary of Commerce

1. Probability of Achieving the Intended Foreign Policy Purpose. Commensurate with the growth of electronic commerce in the world's most developed nations, the number of countries with the

technology to produce highly sophisticated encryption products is growing. This growth is concentrated, however, among nations and trading partners that generally share U.S. security concerns and foreign policy interests. Also, since much of the world's cryptography is supplied by a core group of information security industry leaders, encryption export controls can be very effective in achieving their intended foreign policy purpose. Consistent with E.O. 13026 of November 15, 1996, and the Presidential Memorandum of the same date, the Secretary has determined that these controls achieve the intended purpose of restricting the export of commercial encryption items, in situations in which their export would be contrary to U.S. national security or foreign policy interests.

2. Compatibility with Foreign Policy Objectives. The Secretary has determined that the controls are compatible with the foreign policy objectives of the United States. The controls are consistent with the U.S. foreign policy goal of preventing U.S. exports that might contribute to destabilizing military capabilities or to international terrorist or criminal activities against the United States and its citizens. The controls also contribute to public safety by promoting the protection of U.S. citizens overseas.

3. Reaction of Other Countries. The Secretary has determined that the reaction of other countries to this control has not rendered the control ineffective in achieving its intended foreign policy purpose nor counterproductive to U.S. foreign policy interests. Other allied countries, particularly those with the capability to produce highly sophisticated encryption products, recognize the need to control exports of encryption products for national security and law enforcement reasons. The United States and its key trading and security partners recognize the desirability of securing critical infrastructures, developing new technologies and standards, thwarting cybercrime, and promoting electronic commerce, while restricting goods that could compromise our common security and foreign policy interests. As a result, members of the Wassenaar Arrangement and other international arrangements, such as the European Union, continue to track the U.S. position and implement the multilateral agreements.

4. Economic Impact on United States Industry. The Secretary has determined that the Administration's updated framework for encryption export controls meets the need of U.S. industry to remain the leader in the global market for information security products while continuing to provide essential protections for national security reasons.

In FY 2001, the United States processed 341 license applications for encryption items. The United States approved 243 license applications valued at $31.1 million. These include licenses for exports to government end-users of non-retail items, as well as encryption technology exports, exports civilian end-users in Syria (which is not eligible for license exception ENC), and "deemed exports" of encryption technology for employment of foreign nationals of Cuba, Iran, Iraq, Libya, North Korea, Sudan, or Syria. In addition to these approvals, the United States rejected five applications valued at $65,907 and returned without action 93 applications valued at $67.9 million. Many of these

applications were RWA'd because they qualified for license exception ENC. FY 2001 license levels continue the downward trend that began in FY 2000 when encryption policy was significantly liberalized. In the last fiscal year, 1,094 applications were processed.

Under current encryption policy, most encryption products require a one-time technical review and classification prior to export. In FY 2001, BXA received 983 requests for technical review covering 1,553 controlled encryption products, components, toolkits and source code items. Of the 1,405 encryption products reviewed, nearly 80 percent were classified as "retail" encryption items, making them broadly eligible for export without a license. This compares with 680 applications representing 1,077 encryption items classified last year (from January 14, 2000 when the current encryption policy took effect to the end of FY 2000). Last year 65 percent of encryption products reviewed were made eligible for export as "retail" items.

In addition, in FY 2001, 422 anti-terrorism controlled encryption items (5A992/5D992) were reviewed from 233 requests for classification. BXA also received 241 notifications of encryption items eligible for export pursuant to license exception TSU or ENC.

5. Enforcement of Control. Detection of some encryption transactions is difficult since encryption capability is often incorporated into other products and encryption software can be transferred over the Internet. Conversely, the importance and value of the capability to encrypt data leads to transfers that leave a commercial trail that can be followed. It is easier to enforce controls on proprietary encryption than on "open source" encryption.

C. Consultation with Industry

Since March 1998, and continuing throughout 2001, the Administration has engaged in an intensive dialogue with U.S. industry on encryption policy. The participants in this dialogue have sought to find cooperative solutions that would assist law enforcement, protect national security, ensure continued U.S. technological leadership, and promote the privacy and security of U.S. firms and citizens engaged in electronic commerce. This dialogue has proven successful, as evidenced by the ever-increasing number of encryption items submitted for export review and classification, along with continued industry commitment to assist law enforcement in better understanding current and future technologies.

U.S. firms have overwhelmingly supported the Administration's new export controls framework. Industry provided valuable input on its business models and practices for reporting purposes and other issues during the drafting phase of the regulations. Encryption policy and other information security topics are regularly discussed at conferences, seminars, and meetings with industry.

The President's Export Council Subcommittee on Encryption, met throughout the year to advise the President, through the President's Export Council and the Secretary of Commerce, on matters pertinent to implementing an encryption policy that will support the growth of electronic commerce while protecting public safety, and promoting foreign policy and national security interests. U.S. policy and regulations also reflect consultation with groups such as the Regulations and Procedures Technical Advisory Committee, Alliance for Network Security, Americans for Computer Privacy, and the Computer Systems Policy Project.

On November 7, 2001, the Department of Commerce, via the *Federal Register* and via BXA's Web page, solicited comments from industry on the effectiveness of foreign policy-based export controls. No comments were received specific to the controls described in this chapter. A more detailed review of the comments is available in Appendix I.

D. Consultation with Other Countries

The United States has taken the lead in efforts to prevent international criminals, terrorists and rogue states from acquiring sophisticated encryption products, urging other supplier nations to adopt export controls comparable to those of the United States. As a result, the major industrial partners of the United States maintain their own export controls on encryption equipment and technology. In addition, the United States and the other participants in the Wassenaar Arrangement have established multilateral controls for these items.

The regulations of January 14, 2000, reflect the December 1998 agreement made by Wassenaar members to move encryption items from the Sensitive List to the Basic List, and to make other revisions to encryption controls. This agreement simplified export controls on many encryption products. For example, it created a positive list of controlled encryption products. In the past, the Wassenaar Arrangement required participating countries to control all encryption products without regard to encryption strength. Now, the new list clearly states that products with an encryption key length of 56 bits or less are no longer controlled.

Wassenaar member countries also agreed in 1998 that the General Software Note (GSN) should not apply to encryption. It was replaced with a new cryptography note. The GSN allowed countries to export mass-market encryption software without limits on the key length. The December 3, 1998, modification was essential to close loopholes that permitted the uncontrolled export of encryption with unlimited key length. Accordingly, the agreement set the key length threshold for mass-market products at 64 bits or less. The agreement also extended liberalized mass-market treatment to hardware encryption products. Previously, only mass-market software enjoyed this liberalized treatment. The December 1998 agreement also eliminated requirements to report exports of

encryption products, and removed controls on certain consumer electronic items such as DVD products, personal computer-based media players, and cordless telephone systems designed for home or office use.

E. Alternative Means

The United States has undertaken a range of diplomatic means, both bilateral and multilateral, to encourage other nations to adopt appropriate restrictions on the export of encryption products. Through cooperation with law enforcement officials in friendly countries, the United States has also sought to keep encryption products out of the hands of terrorists and criminals. However, these efforts can only supplement, not replace, the effectiveness of actual export controls.

F. Foreign Availability

The United States recognizes the growing use of encryption overseas, and the continued development of foreign-made encryption hardware and software. The Administration's new encryption framework responds to international marketplace developments to guarantee that U.S. industry can maintain its technological leadership in information security products in a manner that safeguards our national security and public safety interests.

Executive Order 13026 of November 15, 1996, addressed the issue of foreign availability as it relates to encryption items transferred from the USML to the CCL with the following statement:

> "I have determined that the export of encryption products could harm national security and foreign policy interests even where comparable products are or appear to be available from sources outside the United States, and that facts and questions concerning the foreign availability of such encryption products cannot be made subject to public disclosure or judicial review without revealing or implicating classified information that could harm United States national security and foreign policy interests.
>
> Accordingly, sections 4(c) and 6(h)(2)-(4) of the Export Administration Act of 1979, 50 U.S.C. App. 2403(c) and 2405(h)(2)-(4), as amended and as continued in effect by Executive Order 12924 of August 19, 1994, and by notices of August 15, 1995, and August 14, 1996, all other analogous provisions of the EAA relating to foreign availability, and the regulations in the EAR relating to such EAA provisions, shall not be applicable with respect to export controls on such encryption products. Notwithstanding this, the Secretary of Commerce may, in his discretion, consider the foreign availability of comparable encryption products in determining whether to issue a license in a particular case or to remove controls on particular products, but is not required to

issue licenses in particular cases or to remove controls on particular products based on such consideration."

ENDNOTES

1. *E.O. 13026 formally announced the transfer of licensing jurisdiction for encryption items from the Department of State to the Department of Commerce.*