11. Encryption (Section 742.15)

Table of Contents

Export Control Program Description and Licensing Policy

On December 30, 1996, the Bureau of Export Administration (BXA) published in the *Federal Register* (61 FR 68572) an interim rule that exercised jurisdiction over, and imposed new combined national security and foreign policy controls on, certain encryption items, including recoverable encryption "software," that were on the United States Munitions List (USML). This action was taken consistent with Executive Order 13026 (E.O.) and pursuant to the Presidential Memorandum, both issued by President Clinton on November 15, 1996. The Memorandum and E.O. 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 latter items remain on the USML, and continue to be controlled by the Department of State, Office of Defense Trade Controls. In the CCL the acronym "EI" (Encryption Items) designates foreign policy controls on these items.

Since the publication of the interim rule in 1996, export controls on encryption have evolved, with the most recent announcement updating controls being made in September, 1998. The Administration's encryption policy, which Vice President Gore first announced on October 1, 1996, makes it easier for Americans to use stronger encryption products to protect their privacy, intellectual property and other valuable information. The policy relies on market forces to develop a worldwide key management infrastructure with the use of key recovery and recoverable encryption items to promote electronic commerce and secure communications while protecting national security, foreign policy and public safety. The regulations issued in 1996 contained procedures which allowed recoverable encryption products of any strength and key length to be exported under a license exception after a one-time review. In order to encourage the development of these recoverable encryption products, the policy allowed a two-year liberalization period (until January 1, 1999) during which companies were permitted to export non-recoverable encryption items up to 56-bit key length Data Encryption Standard (DES) or equivalent strength, provided the exporter submitted a commitment and business plan demonstrating the intent to develop recoverable encryption products and a global key management infrastructure.

The President's Executive Order directed the Secretary of Commerce to take actions to control the export of technical assistance to foreign persons for the development or manufacture of encryption in the same manner and to the same extent as the export of such assistance is controlled under the Arms Export Control Act. Therefore, the interim rule on encryption prohibits U.S. persons, without a license from Commerce, from knowingly providing assistance to foreign persons, including providing training, to develop or manufacture abroad encryption items transferred from the USML to the CCL. This

provision does not apply to any activity involving items that the U.S Government has authorized under a Commerce license.

Encryption policy is a heavily debated issue, and discussions within, and between, the U.S. Government and the private sector on balancing business and privacy interests with national security, foreign policy and public safety continued throughout 1998. The 105th Congress considered several bills concerning export controls on encryption, none of which were put to a vote on the House or Senate floors. During 1998, the Executive Branch held discussions with industry and privacy advocates to increase the lines of communications among concerned parties.

In May 1997, the United States announced that it would allow the export of the strongest available data encryption products to support electronic commerce around the world. These products included direct home banking software of any key length offered by banks and financial institutions to their customers world-wide. This step was part of the overall Clinton Administration initiative to promote the development of a secure and trusted environment for electronic commerce. In July 1998, Secretary Daley announced that the Clinton Administration had finalized guidelines to allow the export of encryption under a license exception to 45 eligible countries. This affects encryption exports for the world's 100 largest banks and almost 70 percent of the world's financial institutions. On September 22, 1998, Commerce issued regulations implementing these changes.

Furthermore, on September 16, 1998, Vice President Gore announced an update to the encryption policy which was based on input from industry groups but consistent with the protection of national security, foreign policy and law enforcement interests. This update permits the export of strong encryption when used to protect sensitive financial, health, medical, and business proprietary information in electronic form. The new export guidelines further streamline exports of key recovery products and other recoverable encryption products. In particular, for exports of non-recovery 56-bit products, the new guidelines eliminate the requirement for a commitment and business plan to develop key recovery encryption. On December 31, 1998, Commerce issued regulations implementing the encryption policy update. This regulation addresses the closing of the two year window period (January 1996 - December 1998) first announced by Vice President Gore in October 1996.

The President's Export Council Subcommittee on Encryption (PECSENC), which was established in April of 1997, met numerous times throughout 1998 to advise the President, through the President's Export Council and the Secretary, on matters pertinent to implementing an encryption policy that will support the growth of electronic commerce while protecting public safety, foreign policy and national security. The PECSENC is comprised of approximately 30 members from the exporting community, manufacturers, privacy groups and law enforcement officials interested in encryption policy.

A. In general, the United States requires a license for all destinations, except Canada, for exports and reexports of commercial encryption items. However, certain exceptions to the licensing requirements may apply.

B. The United States reviews export license applications for commercial encryption items on a case-by-case basis, to determine whether the export or reexport is consistent with U.S. national security and foreign policy interests.

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

A. The Purpose of the Control

These controls are maintained to protect U.S. national security and foreign policy interests, including the safety of U.S. citizens here and abroad. Encryption can be used to conceal the communications or data of terrorists, drug smugglers, or others intent on taking hostile action against U.S. facilities, personnel, or security interests. Policies concerning the export control of cryptographic products are based on the fact that the proliferation of such products will make it more difficult for the U.S. Government to have access to information vital to national security and foreign policy interests. Also, cryptographic products and software have military and intelligence applications. These controls are consistent with E.O. 13026 of November 15, 1996, and a Presidential Memorandum of the same date.

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

1. Probability of Achieving the Intended Foreign Policy Purpose. Consistent with Executive Order 13026 of November 15, 1996, and a Presidential Memorandum of the same date, the Secretary has determined that the control achieves the intended purpose of restricting the export of commercial encryption items, including products with key recovery features, if their export would be contrary to U.S. national security or foreign policy interests.

2. Compatibility with Foreign Policy Objectives. The Secretary has also determined that the controls are compatible with the foreign policy objectives of the United States. The control is consistent with U.S. foreign policy goals to promote peace and stability and to prevent U.S. exports that might contribute to destabilizing military capabilities and international terrorist or criminal activities against the United States. 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 or counterproductive to U.S. foreign policy interests. Other allied countries recognize the need to control exports of encryption products for national security and law enforcement reasons. These countries also recognize the desirability of restricting goods that could compromise shared security and foreign policy interests.

4. Economic Impact on United States Industry. The Secretary has determined that the transfer of commercial encryption items, including products with key recovery features, from the USML to the CCL benefits industry positively and makes U.S. manufacturers more competitive in the world market. Removal of these products from the USML may actually improve their marketability to foreign, civil end-users who prefer not to trade in items the United States considers to be munitions. Moreover, since key recoverable encryption products pose less security and law enforcement risks, their export has been treated more liberally than export of encryption products with non-recoverable keys. This will allow U.S. manufacturers and exporters to capture a larger share of growing world demand for key recovery-based products.

For FY 1998, BXA received 1753 license applications for encryption items. Commerce approved 1575 applications worth approximately $2 billion, denied 13 applications worth approximately $2 million and returned 165 applications without action worth approximately $378 million.

Some U.S. firms argue that U.S. export controls on encryption hurt their international competitiveness, asserting that encryption products are readily available overseas and that foreign manufacturers are not subject to similar controls. However, these claims do not seem wholly valid for several reasons, including the dominance and superior quality of U.S. encryption products in the world market. Section F below (Foreign Availability) discusses this issue in further detail.

5. Enforcement of Control. The Secretary has determined that the United States has the ability to enforce these controls effectively. Since these items are also under multilateral control, we can expect cooperation from foreign enforcement agencies in preventing violations and punishing violators.

C. Consultation with Industry

On October 13, 1998, the Department of Commerce, via the *Federal Register*, solicited comments from Industry on the effectiveness of export policy. In general, the comments indicated that Industry does not feel that unilateral sanctions are effective. A more detailed review of the comments is available in Appendix I.

The United States consulted with various elements within industry on the recent changes in controls and on the desirability of development of both key recoverable and other types of recoverable encryption products for both Government and industry. Since March of 1998, the Administration has been engaged in an intensive dialogue with U.S. industry on encryption policy. The dialogue was intended to find cooperative solutions that would assist law enforcement, while protecting national security, and would also assure continued U.S. technology leadership and promote the privacy and security of U.S. firms and citizens in electronic commerce. This dialogue was successful, as evidenced by industry's promotion of "recoverable" technologies that advance the interests of law enforcement. Industry has also agreed to assist law enforcement in better understanding current and future technologies.

BXA participates in the deliberations of the PECSENC, which represents a broad cross-section of industry and the public.

D. Consultation with Other Countries

The United States took the lead in international efforts to stem the proliferation of sensitive items, urging other supplier nations to adopt and apply export controls comparable to those of the United States. The major industrial partners of the United States maintain export controls on this equipment and technology. Pursuant to their agreement to establish a new regime for the control of conventional arms and sensitive dual-use technologies, the 33 participants in the Wassenaar Arrangement have agreed to control these items on a global basis and to coordinate export policies for such items. Members of the Organization for Economic Cooperation and Development have agreed to a set of cryptography policy guidelines which allow for the development of a global key management infrastructure.

In addition, the President appointed Ambassador David L. Aaron as Special Envoy for Cryptography and assigned him the responsibility to promote the growth of international electronic commerce and robust, secure global communications in a manner that protects the public safety and national security. As Special Envoy, Ambassador Aaron continued his efforts to lead discussions with major supplier nations on common approaches to encryption policy, including export controls. He has found that most nations have concerns similar to those of the United States regarding encryption. The United States hopes to continue to work together with supplier nations to develop common encryption policies that are compatible and do not hinder development of the emerging information infrastructure.

E. Alternative Means

The United States has undertaken a wide range of diplomatic means, both bilateral and multilateral, to encourage the proper restrictions on these items. However, these efforts can only supplement, not replace, the effectiveness of actual export controls.

F. Foreign Availability

The issue of foreign availability is one that is repeatedly raised in the encryption debate. It is often asserted that encryption products are widely available overseas, that other countries do not control encryption exports, or that U.S. firms are suffering significant losses due to export controls on encryption. These assertions do not appear to be entirely accurate. In 1995, the Department of Commerce and the National Security Agency (NSA) studied the foreign availability of encryption and found that claims of widespread foreign availability of encryption products were inaccurate. Although a number of countries produce encryption products, the issue of foreign availability is complex, and must address the quality of the encryption and the export controls maintained by foreign countries. The United States dominates the worldwide software market, including the market for encryption products. However, U.S. market share is greatest in markets for general purpose software with encryption features; security-specific markets tend to be more national due to national regulations on export and use of encryption. Moreover, it does not appear that U.S. market dominance is seriously threatened, either by export restrictions or commercial factors. . In 1997, there were 656 known encryption products available from sources in 29 foreign countries, as well as 963 domestic products.[1] Germany, the U.K., Canada, and Ireland are the leading producers outside of the U.S. The members of the Wassenaar Arrangement have agreed to control encryption on a multilateral basis; however individual nations' licensing requirements and practices vary (for example, in their treatment of mass-market software exports; treatment of "exports" downloaded from the Internet). As to the quality of foreign encryption, our information indicates that, on the whole, American encryption is superior. However, few if any customers evaluate a product's cryptographic quality prior to purchase. Rather, purchasing decisions are based on price, features, and advertised encryption strength. Some foreign encryption producers use U.S. export controls as a marketing tool for their own products.

In regard to foreign availability as it relates to encryption items transferred from the USML to the CCL, the President's Executive Order of November 15, 1996, stated the following:

> **I have determined that the export of encryption products [transferred to the Commerce Control List] 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.

Table of Contents

ENDNOTES

1. *"Worldwide Survey of Cryptographic Products," Trusted Information Systems, December, 1997*