Return to Table of Contents

10. Encryption (Section 742.15)

Export Control Program Description and Licensing Policy

On December 31, 1998, the United States published an interim rule in the *Federal Register* to implement Vice President Gore's September 1998 encryption export policy announcement. This policy update permits the export of 56-bit hardware and software worldwide to any end-user under a license exception. It also permitted the export, also under license exception of encryption products of 128-bit and higher to banks, financial institutions, health and medical entities, and on line merchants in 46 listed countries, in order to secure their sensitive financial, medical, and on line transactions in digital form. This policy also allowed U.S. companies to export encryption products of 128-bits or higher, including technology, to their overseas subsidiaries to protect their proprietary information and to develop new products.

Further, the December 1998, interim rule permits the export of 128-bit or greater "recovery-capable" or "recoverable" encryption products under an encryption licensing arrangement[1]. Such products include those that are readily available in the marketplace, such as general purpose routers, firewalls, and virtual private networks. These recoverable products are usually managed by a network or corporate security administrator, without any involvement by a third party. The Interim Rule also further streamlined exports of key recovery products by eliminating the requirements for a review of foreign key recovery agents and the submission of company business plans.

Also in December 1998, The Wassenaar Arrangement members agreed to move encryption items from the Sensitive List to the Basic List and to make other revisions to encryption controls. Wassenaar's December agreement was the result of a two-year effort to modernize and improve multilateral export controls on encryption. That agreement simplified export controls on many encryption products (see Section D).

On September 16, 1999, the Administration announced further revisions to encryption export control policy. The new policy provides for information security and privacy protection, a revised framework for export controls and updated tools for law enforcement. It also permits a one-time technical review in advance of the sale of an encryption product, provides streamlined post-export reporting procedures, and lays out a process whereby the U.S. Government reviews the exports of strong encryption to foreign government and military organizations and to entities in nations of concern. The regulation implementing these changes will be published early this year.

The President's Export Council Subcommittee on Encryption (PECSENC), established in April 1997, met six times during 1999 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, foreign policy, and national security. The PECSENC consists of nearly 40 members from the exporting community, manufacturers, privacy groups, and law enforcement officials interested in encryption policy.

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. Among other end-uses, encryption can be used to conceal the communications of 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 foil 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 Executive Order No.13026 of November 15, 1996, and a Presidential Memorandum of the same date[2].

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

1. Probability of Achieving the Intended Foreign Policy Purpose Since the number of countries with the technology to produce highly sophisticated encryption products is small and consists of nations that generally share U.S. security concerns and foreign policy interests, these controls can be very effective in achieving their intended foreign policy purpose. Consistent with Executive Order No.13026 of November 15, 1996, and a 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, including products with key recovery or plaintext-recoverable features, 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 also has determined that the controls are compatible with the foreign policy objectives of the United States. The controls are consistent with U.S. foreign policy goals 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. These countries also recognize the desirability of restricting goods that could compromise our common security and foreign policy interests. As a result, members of The Wassenaar Arrangement have recently reached agreements reflecting the U.S. position.

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

In Fiscal Year 1999, the United States processed 1,749 license applications for encryption items. The United States approved 1,517 applications worth approximately $3.7 billion, denied 20 applications worth approximately $13 million, and returned without action 212 applications worth approximately $202 million. In addition to these license approvals, the United States approved 309 cases for exporting 56-bit or greater encryption items under the license exception ENC. The United States also processed 351 "mass-market" classification requests, which release encryption items from encryption export controls under license exception "technology and software unrestricted" (TSU).

C. Consultation with Industry

Beginning in March 1998 and continuing throughout 1999, the Administration has been engaged in an intensive dialogue with various elements of 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 industry's promotion since 1998 of "recoverable" technologies that advance the interests of law enforcement, and its 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.

In addition to these outreach efforts, Commerce 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 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 and supply 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 32 other participants in The Wassenaar Arrangement have established multilateral controls for these items on a global basis.

In December 1998, Wassenaar members agreed 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.

Also in 1998, Wassenaar member countries agreed 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 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 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 3 agreement also eliminated requirements to report exports of encryption products, and removed controls on certain consumer electronic items such as DVD products and cordless telephone systems designed for home or office use. The United States will publish an implementing regulation early this year.

E. Alternative Means

The United States has undertaken a wide 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.

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 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 No.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.

Therefore, the foreign availability provision does not apply to items determined by the Secretary of State to require control under Sections 4(c) and 6(h)(2)-(4) of the Export Administration Act.

ENDNOTES

1. *This encryption licensing arrangement allows the export of unlimited quantities of a company's product to a certain category of destinations (for example, banks).*

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