11. Encryption (Section 742.15)

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 exercises jurisdiction over, and imposes 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), consistent with Executive Order 13026 and pursuant to the Presidential Memorandum of that date, both 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 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.

The Administration's encryption policy, which was first announced by the Vice President 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 encryption items to promote electronic commerce and secure communications while protecting national security and public safety. The regulations contain procedures which allow 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 allows a two-year liberalization period (until January 1, 1999) during which companies may export non-recoverable encryption items up to 56-bit key length Data Encryption Standard (DES) or equivalent strength, provided the exporter submits a commitment and business plan demonstrating the intent to develop recoverable encryption products and a global key management infrastructure.

The President's Executive Order directs the Secretary of Commerce to take actions to control the export of assistance to foreign persons 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 manufacture or to export encryption items transferred from the USML to the CCL. This provision does not apply to any activity involving such encryption items that have been licensed or otherwise authorized by Commerce.

During 1997, encryption policy has been a heavily debated issue. New topics in the debate have prompted discussion on revisions to the regulations. Pending amendments to the regulations

will address the issue of banks and financial institutions.

In May 1997, the Department of Commerce announced that it would allow the export of the strongest available data encryption products to support electronic commerce around the world. These products include direct home banking software of any key length, offered by banks 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. The products and institutions that will make up a robust security infrastructure will permit users from homes and businesses to perform all types of commercial data transactions, ranging from managing investment transactions to purchasing goods and services. That infrastructure will manage encryption and digital signature keys to provide privacy, message integrity, user authentication, and recovery services. Because banks and other financial institutions are subject to explicit legal requirements and have shown a consistent ability to provide appropriate access to transaction information in response to authorized law enforcement requests, key recovery will not be required for certain financial-specific products.

In addition, on April 24, 1997, the Secretary of Commerce established the President's Export Council Subcommittee on Encryption, comprising forty members from the exporting community, manufacturers and law enforcement officials interested in encryption policy. The Subcommittee will 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 the public safety and national security

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

C. Exporters of 56-bit DES or equivalent encryption products are required to make commitments to develop and market products that support key recovery. The Administration believes that the worldwide use of key recovery encryption products will promote secure international networks for electronic commerce, while protecting national security and public safety.

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

A. The Purpose of the Control

The purpose of the control is 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.

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 denying 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.

From December 30, 1996, through September 30, 1997, BXA received 1,488 license applications containing encryption items. During this period, 1,075 of these applications were approved, valued at $3.3 billion, and 20 applications were rejected, worth $1.1 million. There were 97 applications returned without action, valued at $238 million. The remaining cases were

still pending at the end of FY 1997.

Forty companies have submitted commitment plans which lay out how they will build and market key recovery products. These companies include some of the largest software and hardware manufacturers in the United States. BXA has approved 32 of these plans; none have been rejected. Furthermore, eight companies have submitted requests for a one-time review of key recovery encryption items which will facilitate the establishment of a key management infrastructure (KMI). Four of these products have been approved for eligibility under License Exception KMI. BXA has also approved four U.S. entities to serve as their own Key Recovery agents for these products (i.e., corporate "self-escrow").

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 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. U.S. controls on this product and technology have been transferred from the State Department's Munitions List to the Commerce Department's Commerce Control List. Commerce Department is making manufacturers and dealers aware of the transfer of authority, and that the items covered by this transfer are under strict control. The strategic importance of these items is clear. Finally, 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

The United States consulted with various elements within industry on the proposed change in controls and on the desirability of development of key recoverable encryption products for both Government and industry. During the first two months of 1997, the Department of Commerce received industry comments to the December 30, 1996, published rule. These comments included general concerns and objections to the policy embodied in the regulations, recommendations for specific changes or clarifications to the regulations that are consistent with the broad encryption policy implemented in the December 30 rule, claims that no market presently exists for key recoverable features, and recommendations for additional changes to encryption policy. These comments were made available to the general public on the Bureau's web site. The Bureau continues to seek comments from industry sectors affected by encryption export controls, and takes these views into account in its internal deliberations on changes to encryption regulations and policy.

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, with 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 has led discussions with major supplier nations on common approaches to encryption policy, including export controls. He has found that most of the nations have concerns similar to those of the United States regarding encryption. The United States hopes 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

Alternatives to export controls at this time would not be the most effective means of achieving the intended national security and foreign policy objectives. 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. The United States dominates the worldwide software market, including the market for encryption products. Moreover, it does not appear that this dominance is threatened, either by export restrictions or commercial factors. While 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 members of the Wassenaar Arrangement have agreed to control encryption on a multilateral basis. As to the quality of foreign encryption, our information indicates that, on the whole, American encryption is superior.

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.