# Testimony
# Honorable William A. Reinsch
# Under Secretary of Commerce

## *New Directions in Commercial Encryption Policy*

**Senate Commerce Committee**
**July 25, 1996**

**GO TO:**


Dealing in a balanced fashion with the spread of encryption is one of the most difficult public policy issues we face today. Our response must address three important interests: law enforcement, national security and our commercial and privacy interests. I would like to provide some comments on how the Administration's policy balances those interests, the results of our study of the global encryption market, and our view of S. 1726, which is pending before the Committee.

Making strong commercial encryption widely available is in the best interest of the United States. Indeed, it is inevitable, as we learn to exploit the advantages of powerful computers and advanced telecommunications. These technologies are rapidly leading to the creation of broad electronic networks which will form the basis for communication and commerce in the future. The ability to encrypt electronic messages and data will be essential for electronic commerce and for the full development of information technology. Businesses and individuals need encrypted products to protect sensitive commercial information and to preserve privacy, and their demand for those products will further facilitate the spread of encryption.

This trend is also economically desirable. Protecting the confidentiality of business information will reduce losses from industrial espionage. Perhaps more important, we are the world's leading producer of information technology with almost half of the world's producers, and roughly half their revenues come from exports.

To retain this leading position and the substantial benefits to our economic health it produces, we must ensure our producers' continued ability to capture foreign market share. Our companies must be able to meet the growing demand for products with strong encryption. If they do not, foreign firms will ultimately step in to fill the void. The United States' policy on encryption must advance the interests of this vital industrial sector. We must shape our export control policies to allow American companies to take advantage of their strengths in information technology in their pursuit of global markets.

Our problem arises from the fact that the increased use of encryption carries with it serious risks. The spread of powerful encryption products poses very real problems for law enforcement and for our national security -- as my colleagues have testified. Any policy on encryption must address these risks if it is to be in the national interest. The Clinton Administration is making a very serious effort to develop a policy that balances the expanded availability of the strong encryption needed for economic growth and individual privacy with our national security and law enforcement needs. Most important, we are attempting to do that in close consultation with our allies and the private sector and by working with the market, not against it.

**The Administration's Approach**

We have been working with industry to develop a framework, based on a key management infrastructure which would allow government to recover the key where necessary. This will encourage the use of strong encryption while protecting law enforcement and national security interests. This framework will be developed and implemented by industry, not the government, and would be available for both domestic and international use. Participation in it will be voluntary, and Americans will continue to be free to use any encryption they choose in the United States. This approach clearly differs from previous efforts, such as "Clipper Chip," which contemplated a dominant role for government. Our approach takes the opposite tack -- a limited government role working with industry to develop supply and demand for products that will operate in a key management environment. The federal government will work with industry to set standards for federal use of these products, establish criminal and civil liability for improper certification or release of keys, provide a market through purchases for government agencies, encourage the development of pilot projects, and negotiate with our trading partners on a common approach to encryption. We will not dictate the scope or style of the infrastructure, nor the encryption used within it.

This infrastructure will be based upon trusted parties who will hold keys to confidential data. In some cases, corporations would hold their own keys if they are willing to meet law enforcement requirements; in other cases, users might choose to use key recovery services provided by trusted third parties. These trusted third parties will be private entities. Access to the keys would be provided only to the owners where they have lost or damaged their own key or to law enforcement officials acting under the authority of the courts. This approach balances economic needs with law enforcement concerns and is one that many of our major trading partners, most notably the United Kingdom, are also adopting. The United States is working bilaterally and in the OECD to develop an international framework for a key management infrastructure that will ensure equal protection for consumers and equal access to markets for producers. Our view is that a global key management infrastructure provides the best means of using strong encryption in a responsible manner.

We have come to this view after a great deal of work, one element of which I would like to mention -- a study done jointly by the Bureau of Export Administration and the National Security Agency.

**Background and Purpose of the Encryption Study**

Computer software and hardware companies believe that current encryption export controls are outdated and ineffective and are causing them to lose their global competitiveness. They assert there are a multitude of strong foreign encryption products available. In late 1994, in fulfillment of Vice President Gore's earlier commitment, National Security Advisor Anthony Lake directed that a report be prepared assessing the current and future international market for software products containing encryption and the impact of export controls on the U.S. software industry.

The Department of Commerce and the National Security Agency jointly prepared the report, which was completed in July, 1995. The Bureau of Export Administration took the lead in assessing domestic and international markets for encryption and the impact of export controls on U.S. industry, while NSA was responsible for identifying and evaluating foreign encryption software products and international laws and controls governing use, export and import of encryption. A declassified version of the final report was made available to the public in January 1996.

**Methodology and Industry Involvement**

A wide variety of government agencies, academic experts, commercial information sources, trade associations, and industry representatives were contacted. No definitive statistics exist regarding the size and composition of the U.S. market for encryption software. BXA consulted with computer security specialists, market researchers, and academics to create a picture of the current and future domestic market for these products. We supplemented this information with an informal poll of information security specialists from ten diverse Fortune 500 companies to determine how these firms are currently using encryption software.

To assess the international market, BXA utilized the Foreign Commercial Service in 31 U.S. embassies. They provided input on demand for encryption in their host countries as well as the estimated U.S. share of the market. U.S. officials overseas and foreign government officials provided information on foreign laws, regulations, and policies affecting encryption. We used this information to determine the extent to which regulatory controls influence the international marketability of encryption software products.

Foreign encryption software products were identified and purchased for review. NSA cryptanalysts studied the 28 foreign products ultimately obtained to evaluate their strengths and weaknesses. Finally, in order to determine the impact of existing export controls on U.S. software vendors, BXA worked closely with the Software Publishers Association, Business Software Alliance and other industry groups to develop an industry questionnaire. The voluntary questionnaire was mailed to about 200 firms believed to be involved in the encryption software market. It was also posted on the Internet. Thirty six encryption software producers elected to respond to the questionnaire, which gave them an opportunity to explain and quantify the impact of export controls on sales, employment, profitability, and product development. Frankly, this was a disappointing response, despite repeated appeals to the industry, and it has led us to the conclusion that many companies are unwilling or unable to quantify the effects of controls on their operations.

**Major Findings**

Let me summarize some of our major findings:

- All countries that are major producers of commercial encryption products control exports to some extent, but licensing practices and policies vary significantly. A few countries, notably France, Russia, and Israel, also control imports and/or domestic use of encryption. Some countries in Europe and elsewhere apparently treat exports to the United States of DES-based software more liberally than the United States treats DES exports to those countries, as evidenced by our ability to procure products purportedly using DES. The U.S. generally allows export of DES-based products only for financial institutions.
- While encryption software currently accounts for only a small percentage of the total software market (1-3%), we expect the future growth trend to be great. The overwhelming majority of general purpose software products (such as word processors, database programs, etc.) with encryption capabilities available in U.S. and foreign markets are of U.S. origin. The U.S. presently has few viable foreign competitors in this market. The vast majority of these products can be exported without prior U.S. government authorization because they incorporate weaker encryption algorithms (40 bits or less).

  In the security-specific software market, however, U.S. manufacturers face competition in foreign markets from countries such as the United Kingdom, Germany, and Israel. To a large extent, markets for these products tend to be "national," with local vendors capturing a large portion of their home markets, in part due to the influence of export controls. In many foreign countries surveyed, exportable U.S. encryption products are perceived to be of insufficient strength. In about half the countries, overseas sources believe that U.S. export controls have limited U.S. market share. Some maintain that U.S. export controls promote indigenous production of encryption software.

- In the absence of significant foreign competition, the effect of export controls on general purpose software producers has been minimal so far. For these products, customers tend to base purchasing decisions on the primary function of the software (spreadsheet, word processing), not on encryption features. The vast majority of general purpose products are specifically designed with encryption algorithms to be eligible for export. Export controls have, however, affected the plans of general purpose software manufacturers to enhance encryption capabilities to meet anticipated demand. They fear that their foreign competitors may attempt to use encryption features to differentiate their products and capture market share.
- Many domestic security-specific software producers are restricted to the U.S. market because of export controls. Since security is the primary function of their products, it is not feasible for them to utilize weaker encryption algorithms that could be exported. These companies believe that there is potential for significant foreign sales, but they are unable to quantify it since they do not market overseas. Moreover, there is a widespread perception among foreign purchasers that strong U.S. products may not be exported, and that exportable U.S. products are unsatisfactory. This perception serves to dampen demand for U.S. products.

- The existence of foreign products advertising DES or other strong encryption has damaged U.S. competitiveness domestically and abroad, regardless of the accuracy of those claims. Some U.S. companies either use or consider using foreign encryption products to communicate worldwide with their customers, suppliers and international partners.

**Next Steps**

Our study encouraged us to move ahead with the new approach I mentioned. This policy is based on key recovery, but it will be a flexible approach developed by and based in the private sector. Cooperation with industry is critical, and we are finding a willingness among many firms to work together toward a solution. As it will take some time to complete development of this new approach, we are considering a number of interim measures to ease the burden on industry while it moves to a key management infrastructure. In the expectation of industry cooperation in that regard, the Vice President on July 12 indicated what these measures might include:

- Liberalizations of existing export controls for certain commercial encryption products.
- Pilot management programs to test key recovery with industry and with our trading partners.
- The creation of a private sector advisory committee to develop performance and technical standards for products the government will purchase.
- And, possibly, the transfer of jurisdiction for commercial encryption products from the Department of State to the Department of Commerce.

Our work is not yet done. We are continuing to consult with industry and international partners to refine our proposal, and we plan to send recommendations to the President this September. Our goal is to develop a flexible, market-driven approach that balances public safety, national security, and economic vitality.

In the midst of this effort, legislation such as S. 1726 would not be helpful. Its fundamental flaw is that it does not provide the balanced approach we are seeking and instead would unnecessarily sacrifice our law enforcement and national security needs. Legislating decontrol of encryption would destroy any hope of developing a consensus on policy; it would be greeted with dismay by our international partners; and it would pose real risks to the safety of Americans.

In addition, from the perspective of the Commerce Department, we have a host of specific concerns about the bill. In particular, we believe it misunderstands and misstates the role of NIST in regulation and standard-setting. NIST is not a regulatory agency and does not "regulate" or control private sector use of encryption. It prepares

and recommends to the Secretary for approval Federal Information Processing Standards (FIPS), which are intended to assist government agencies and are developed in consultation with the private sector. Often these standards, of which DES is one, have been adopted and utilized by the private sector in the interest of standardization -- an important objective in this sector but one which will be determined by the market rather than the government. The private sector has consistently been supportive of NIST's efforts in this area, and it is difficult for us to understand why the authors of S. 1726 would want to preclude that cooperation.

As I said when I began my remarks, encryption is one of the most difficult issues in public policy today, but it is a problem which this Administration is committed to solving in cooperation with industry in a way that reinforces market principles and achieves our varied goals. We hope that Congress will work with us to facilitate that process rather than obstruct it by passing unnecessary and harmful legislation.