Testimony
Honorable William A. Reinsch
Under Secretary of Commerce

Administration Encryption Policy

Senate Commerce Committe

March 19, 1997

Go to: Administration Policy | Next Steps

Mr. Chairman, much has happened since my last appearance before this Committee last July 25th. The President has decided on an encryption policy, and we are well on our way to implementing it. It is designed to balance the competing interests I discussed when I was here last: privacy, electronic commerce, law enforcement, and national security.

Making strong commercial encryption widely available is in the best interest of the United States. Indeed, it is inevitable, as powerful computers and advanced telecommunications rapidly lead 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 the world's producers and roughly half their revenues coming from exports. And we want to keep it that way.

To retain this leading position and the jobs 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 step in to fill the void. The United States cannot allow its encryption policy to become a point of vulnerability for 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.

But the increased use of encryption carries with it serious risks for law enforcement and our national security. Any policy on encryption must address these risks as well if it is to be in the national interest. Our policy provides that balance, and does it in close consultation with the private sector and by working with the market, not against it.

The Administration's Policy

The President's policy of balance is based on trying to promote key recovery in the marketplace. By "key recovery" I refer to a range of technologies, some in existence, some under development, some still being conceived, designed to permit the plain text recovery of encrypted data or communications. There has been a tendency in this debate to construe this term and others as narrowly focussed on a single technology, and I want to make clear that is not our intent. We expect the market to make those judgments. In order to facilitate the development and dissemination of these products, we have taken the following steps:

On December 30, 1996, we published new regulations that transferred the licensing of commercial encryption products from the Department of State's Munitions List to the Department of Commerce's Dual-Use list. This change of jurisdiction emphasized the Administration's decision that strong encryption is not something to be used primarily by governments or military forces, but will become an accepted part of normal commercial activity.

The new regulations set forth several procedures which support the development of a key management infrastructure. The most important of these is the creation of a license exemption which would allow recoverable encryption products of any strength and key length to be exported freely after a single review by Commerce, Justice and the Department of Defense.

We have also expanded the definition of products eligible for this key recovery license exemption to include not only "key escrow" systems, which use a trusted third party, but also other systems which allow for recovery of the keys or plain text. This means that we have gone beyond a simple prescription for key escrow and trusted third parties as the solution to all encryption needs.

The new regulations also allow for self-escrow and escrowing of keys overseas in certain circumstances, which will make key recovery products more attractive in export markets. Since the establishment of a key management infrastructure may take some time, the regulations make explicit that we will consider requests for self escrow and escrowing overseas even before there are government agreements on access or an established network of recovery agents in place.

To encourage the movement toward the development of these recoverable encryption products, we have also created a special, two year liberalization period during which companies may export 56 bit DES or equivalent products, provided they submit plans and show that they are working to develop the key management infrastructure envisioned by the Administration. This temporary relief will help provide an incentive and a transition period for manufacturers to move to Key Management Infrastructure.

To help create standards which will guide the Federal Government in its own encryption key management efforts, the Department of Commerce has formed the "Technical Advisory Committee to Develop a Federal Information Processing Standard for the Federal Key Management Infrastructure." This committee will advise the Secretary of Commerce on the development on standards for use by federal agencies for the recovery of

their encrypted information. These standards could also be used by the private sector on a voluntary basis. We believe this Committee activity is consistent with the 1996 National Research Council recommendation that the government explore escrowed encryption for its own uses. The Committee, which has met twice, has been briefed by representatives of six foreign governments, to help ensure coordination and compatibility on a multilateral basis.

In addition, we have continued discussions with our major trading partners on a common approach to encryption policy. To head this effort, the President appointed David Aaron, our Ambassador to the Organization for Economic Cooperation and Development as his Special Envoy on Encryption. His testimony today will discuss the progress we have made.

We also asked for public comments on this new regulation. We received 43. They are posted on BXA's web site for all to review. A few are critical, but many are very helpful. Perhaps a better gauge of industry response has been the flow of applications since the change in policy. In the first two months we have received close to 400 license applications for exports valued at almost $500 million. Twelve companies have submitted commitment plans which lay out how they will build and market key recovery products, and we know that others are preparing them. These twelve companies include some of the largest software and hardware manufacturers in the country. We have approved six of these plans, and we expect to approve more very shortly.

The flow of licenses and the company commitment plans tell us our policy is working. That said, we intend to amend our regulations in the near future to reflect the many helpful comments we received from industry. We want to make sure that our efforts to regulate the export of recoverable encryption are compatible with the larger structure for electronic commerce now beginning to take shape.

We have also supported the development of ten pilot projects designed to demonstrate key recovery in such diverse applications as processing electronic grants and sharing international patent applications. I have with me a description of those projects, and I would request that it be included in the record.

Next Steps

The Administration has stated on numerous occasions that we do not support mandatory key escrow and key recovery. Our objective is to enable the development and establishment of a voluntary key management system for public-key based encryption. We believe the Administration's policy is succeeding in bringing key recovery products to the marketplace. Our attention is now turning toward how we can best facilitate the development of the key management infrastructure that will support those products. To that end, we will shortly submit legislation intended to do the following:

-- Expressly confirm the freedom of domestic users to choose any type or strength of encryption.

-- Explicitly state that participation in the key management infrastructure is voluntary.

-- Set forth legal conditions for the release of recovery information to law enforcement officials pursuant to lawful authority and provides liability protection for key recovery agents who have properly released such information.

-- Criminalizes the misuse of keys and the use of encryption to further a crime.

-- Offers, on a voluntary basis, firms that are in the business of providing public cryptography keys the opportunity to obtain government recognition, allowing them to market the trustworthiness implied by government approval.

In reviewing the pending bills, S. 376 and S. 377, let me say first how much we appreciate the diligence of Senators Leahy and Burns in trying to bring the various parties together to reach a common view. We welcome that and urge them to continue such efforts.

At the same time, I must tell you that legislation such as S. 377 would not be helpful, and the Administration cannot support it. It does not provide the balanced approach we are seeking and as a result would unnecessarily sacrifice our law enforcement and national security priorities. I defer to other witnesses to describe the impact of the bill on law enforcement, but let me describe a few of its other problems.

-- The bill appears to decontrol even the strongest encryption products. By limiting licensing requirements to military and terrorist activities, the bill severely limits government review of highly sensitive transactions. Further, by greatly restricting regulatory authorities, the unintended effect of the bill might be to slow the development of electronic commerce by retarding the creation of standards, even when they are sought by the business community.

-- Whether intended or not, we believe the bill as drafted would preclude the development of key recovery even as an option. The Administration has repeatedly stated that it does not support mandatory key recovery, but we most certainly endorse and encourage development of voluntary key recovery systems, and we see a strong and growing demand for them that we do not want to cut off.

-- From the perspective of the Commerce Department, we also have a host of specific concerns about the bill. We believe, in particular, that it misunderstands and misstates the role of NIST in regulation and standard-setting. NIST does not "regulate" the use of encryption products by U.S. industry. It prepares and issues Federal Information Processing Standards (FIPS), which apply only to government agencies and are developed in consultation with the private sector. Often these standards, of which DES is one, have been voluntarily adopted and utilized by the private sector in the interest of standardization. This is an important objective in the private sector, but it is one which will be determined by the market rather than the government. The private sector has consistently been supportive of NISTs efforts in this area, and it is difficult for us to understand why the authors of this bill would want to preclude them.

-- In contrast, Senator Leahy's bill, S. 376, has a number of similarities to what we will shortly submit, but it also proposes export liberalization far beyond what the Administration can entertain and which would be contrary to our international export control obligations. The Administration has a long-standing policy that the risks to national security and law enforcement which would arise from widespread decontrol of encryption justify continued restrictions on exports. We are sympathetic to the overall objective of the bill, including criminal and civil penalties for unauthorized release by key holders, but we have concerns about the bill's guidelines and standards for establishment of a key recovery system.

As I said when I was here last, Mr. Chairman, encryption is one of the most difficult issues in public policy today, but we are committed to solving it in cooperation with industry, the law enforcement community and the Congress in a way that reinforces market principles and achieves our diverse goals. We hope that you will work with us to facilitate that process by passing the legislation we are proposing.