

**Testimony Of**

**THOMAS PARENTY**

**DIRECTOR, DATA/COMMUNICATIONS SECURITY**

**SYBASE, INC.**

**On Behalf Of The**

**BUSINESS SOFTWARE ALLIANCE**

**IMMEDIATE NEED FOR EXPORT CONTROL RELIEF FOR  
SOFTWARE WITH ENCRYPTION CAPABILITIES**

**Before The**

**COMMERCE COMMITTEE**

**U.S. HOUSE OF REPRESENTATIVES**

**Washington, D.C.**

**September 4, 1997**

**SUMMARY OF STATEMENT OF THOMAS PARENTY**

**DIRECTOR, DATA/COMMUNICATIONS SECURITY, SYBASE, INC.**

**Export controls of software and hardware with encryption capabilities must be immediately modernized.** Export control relief is necessary to enable American software companies to remain competitive internationally; provide users worldwide with the tools to protect their sensitive, confidential electronic information; and continue leading the development of the Global Information Infrastructure.

**The computer software industry is an American success story. It is one of the country's fastest growing and most internationally competitive industries.** Our mass market software products currently have a 70% worldwide market share.

**But existing unilateral U.S. export controls on software with encryption capabilities directly threaten to end this story.** American software companies have been forced to limit the strength of their encryption to a 40-bit key limit set in 1992 despite the fact that:

- The world standard for currently deployed systems with encryption is DES with 56-bit keys. The minimum strength now required by new Internet applications is 128-bit key encryption.
- 40 bit encryption is widely acknowledged to be vulnerable to commercial attack.

**Foreign manufacturers now provide 128-bit encryption alternatives and add-ons – filling the market void created by U.S. export controls.**

**Importantly, the recent National Research Council's CRISIS Report provides critical independent support for export control relief.**

**The Administration's "new" policy is no solution. It does not offer real export control relief; instead, it is an attempt to use export policy to control the domestic use of encryption.**

- It does not permit the easy exportability of 56-bit encryption products as called for by the NRC. Companies may export products with longer key lengths only if they provide the encryption key or other decryption means in advance to a government approved third party.
- It relies upon an unproven, unbuilt and inherently imperfect key recovery-based "key management infrastructure" for use of encryption in a mass market context.
- It is flawed and self-defeating because it is not market-driven and user-based. It requires key recovery for communications as well as stored data despite the lack of commercial demand.

**But the government will only obtain the access it seeks if American companies widely deploy data recovery products that consumers will actually purchase and use.** Consumers, both domestic and foreign, will not adopt a mandated, Administration-designed, top-down, one-size-fits-all solution.

**Thus, BSA strongly supports the SAFE Act (H.R. 695) because it provides badly needed export control relief.** The SAFE Act recognizes that the United States should not try to control uncontrollable exports of mass market and public domain software. It also permits the export of at least DES-level custom software and hardware products. At the same time, the SAFE Act prohibits mandatory key escrow/recovery. Ultimately, the SAFE Act will help Americans to use encryption to prevent crime and to protect our national security.

## **Introduction**

Good Morning. My name is Thomas Parenty, and I am the Director of Data and Communications Security for Sybase, Inc. In this capacity, I am responsible for all security-related product development for the sixth largest software company in the world. I have been active in the cryptography and computer security field for over a decade, starting with my tenure at the National Security Agency (NSA) in the early to mid-eighties.

While at the NSA, I advised the Director of the NSA on internal NSA computer security issues and worked on the security of global nuclear command and control networks, focusing on the formal verification of cryptographic protocols and internal computer security controls. Because of my specialized security knowledge, I worked on national security-related, compartmented programs at other government agencies during my service at the NSA. In addition, I have worked on the security design of operating systems, networks and database management systems for government agencies, including

the Central Intelligence Agency, the Defense Intelligence Agency, the Air Force, as well as many U.S. computer vendors. Most recently, I have been serving as an advisor to the President's Commission on Critical Infrastructure Protection, specifically addressing the needs of the telecommunications and banking infrastructures.

Headquartered in Emeryville, California, Sybase, Incorporated, is a worldwide leader in distributed, open computing solutions with record revenues in 1996 of over \$1 billion. We provide customers and partners with the software and services to create business solutions for strategic, competitive advantage. These high-performance, end-to-end solutions encompass client/server, Internet and intranet transaction processing and data mart and data warehousing applications. Sybase's Adaptive Component Architecture™ enables rapid design, development and deployment of distributed multi-tier business applications. Our product lines include Sybase high-performance database servers, EnterpriseConnect™ distributed data access and connectivity products, and Powersoft open business development tools.

I greatly appreciate the opportunity to appear today before this Committee on behalf of Sybase and the Business Software Alliance (BSA). The BSA promotes the continued growth of the software industry through its international public policy, education, and enforcement programs in 65 countries throughout North America, Europe, Asia and Latin America. BSA worldwide members include the leading publishers of software for personal computers, including Adobe, Apple Computer, Autodesk, Bentley Systems, Lotus Development, Microsoft, Novell, The Santa Cruz Operation and Symantec. BSA's Policy Council consists of these software publishers and other leading computer technology companies, including Intel, Compaq and my company Sybase.

But we really are here today to speak on behalf of the tens of millions of users of American software products. The American software industry has succeeded because we have listened and responded to the needs of computer users worldwide. We develop and sell products that users want and for which they are willing to pay.

One of the most important features computer users are demanding is the ability to protect their electronic information and to interact securely worldwide. American companies have innovative products which can meet this demand and compete internationally. But there is one thing in our way – the continued application of overbroad, unilateral, export controls by the U.S. Government.

The Security and Freedom through Encryption (SAFE) Act, H.R. 695, modernizes export laws regarding software and hardware with encryption capabilities to permit American companies to compete on a level international playing field and to provide computer users with their choice of adequate protection for their confidential information.

For these reasons, BSA strongly supports the SAFE Act, and we thank the members of the Committee who have joined the majority of the full House of Representatives as cosponsors (approximately 250 and growing). BSA also urges the Committee to report

the SAFE Act unamended as it was reported by both the House Judiciary and International Relations Committees.

## **Users – Individuals, Companies, and Governments – Are Demanding Strong,**

### **Secure Networking Systems**

American individuals and companies are rapidly becoming networked together through private local area networks (LANs), wide area networks (WANs) and public networks such as the Internet. Combined, these private and public networks are the economic engine driving electronic commerce, transactions and communications. This engine is being choked by the lack of availability of strong encryption products.

Companies, governments and individuals are now realizing that they can no longer protect data and communications from others by relying on limiting physical access to computers and maintaining stand-alone centralized mainframes. Companies and individual users are demanding the ability to use encryption to protect their electronic information and to interact securely worldwide. They do not want to put sensitive personal information and confidential business information online without this protection. In 1996 the Computer Security Institute/FBI Computer Crime Survey indicated that our worldwide corporations will be increasingly under siege: over half from within the corporation, and nearly half from outside of their internal networks.

Governments also are recognizing that without encryption, the electronic networks that control such critical functions as airline flights, health care functions, electrical power and financial markets remain highly vulnerable. The U.S. General Accounting Office in its report issued in May of 1996 entitled "*Information Security: Computer Attacks at Department of Defense Pose Increasing Risks,*" found that:

- Computer attacks are an increasing threat, particularly through connections on the Internet;
- Such attacks are costly and damaging; and
- Such attacks on Defense and other U.S. computer systems pose a serious threat to national security.

For these reasons, the interests of computer users, hardware and software companies and privacy groups, are not opposed to those of law enforcement and national security. As the blue ribbon National Research Council (NRC) Committee found in its May 1996 CRISIS Report ("Cryptography's Role in Securing the Information Society"), encryption prevents crime by protecting the trade secrets and proprietary information of businesses and correspondingly reducing economic espionage. Encryption also promotes the national security of the United States by protecting "nationally critical information systems and networks against unauthorized penetration."

Thus, the NRC Committee found that on balance the advantages of more widespread use of encryption outweighed the disadvantages and that the U.S. Government has "an

important stake in assuring that its important and sensitive . . . information . . . is protected from foreign government or other parties whose interests are hostile to those of the United States."

Information security is critical to the integrity, stability and health of individuals, corporations and governments. While cryptography is but one element of security, it is the keystone of secure distributed systems. Frankly, there is no substitute for good, widespread, strong cryptography when attempting to prevent crime through these networks. For these reasons, corporations are now demanding 128-bit encryption.

American companies do have exciting and innovative products that can meet this demand and compete internationally. But unless the current unilateral U.S. export restrictions are changed to allow the use of strong encryption, American individuals and businesses will not be active participants in this new networked world of commerce – let alone continue to be the leaders in its development. Furthermore, American companies will no longer be providing the world with the answers to their security problems. Instead foreign nations will. It is unclear how U.S. national security or law enforcement will be aided when foreign encryption products dominate the world market.

**Modernized Export Controls for Products with Encryption Capabilities Are Critical to the Continued Success of U.S. Software and Hardware Companies in the Worldwide Market**

*America's software and hardware industries are important contributors to U.S. economic security – now and in the future.* The incredibly dynamic U.S. computer software industry is an American success story. Between 1980 and 1992, the computing and software industry grew at an annual rate of over 28%, while overall domestic growth was less than 3%. From 1990 through 1996, the software industry grew at a rate of 12.5%, nearly 2.5 times faster than the overall U.S. economy.

Today, the software industry employs 620,000 in the United States, having doubled employment between 1988 and 1994, and created 60,000 new jobs in 1995 alone. Combined, the computing, software and semiconductor industries account for over 1.2 million jobs. This is larger than all but five manufacturing industries.

Moreover, the computer software industry has achieved tremendous success in the international marketplace. American produced software accounts for 70% of the world market, with exports of U.S. programs constituting half of the industry's output. The incredible growth of the industry and its exporting success benefits America through the creation of jobs, highly-skilled, well-paid jobs, here in the United States.

*Unilateral U.S. export controls are out of touch and are harmful to America's software and hardware industries.* Currently, there are no restrictions on the use of cryptography within the United States. However, the U.S. Government maintains strict unilateral export controls on computer software that offers strong encryption capabilities. Therefore, while we can provide programs with strong encryption to customers in the United States,

we cannot sell those same programs overseas. This is problematic for users as the Internet is meant to provide users (individuals, small businesses and leading corporations) with the ability to interact globally for a fraction of the previous cost. But they cannot do so in a secure manner. This is also problematic for U.S. software companies because of the marketing difficulties in selling foreign purchasers a weaker version of an encryption product as well as the additional cost of developing and selling two versions of a program worldwide.

American software companies have been forced to continue limiting the strength of their encryption to a 40-bit key length level set in 1992 – despite an Administration commitment at that time to increase key lengths regularly to take into account technological and market developments. Recently regulations provide that on a company-by-company basis, the Administration will allow export products with 56 bit encryption capabilities – but only in exchange for proof of commitments to build "key recovery" into future products. However, the Administration wants to define "key recovery" in its own terms, not in consumer-driven terms, and the licenses are not easy to get. This policy ignores the fact that:

- The world standard for currently deployed systems with encryption is DES with 56-bit keys. The minimum strength now required by new Internet applications is 128-bit encryption;
- The most widely used encryption program, PGP, with over two million users worldwide, uses the Swiss developed IDEA encryption algorithm, with a 128-bit key;
- Foreign manufacturers now provide 128-bit encryption alternatives and add-ons – filling the market void created by U.S. export controls; and
- 40 bit encryption is widely acknowledged to be vulnerable to commercial attack.

***As a result, encryption expertise is being developed off-shore by foreign manufacturers who now provide hundreds of encryption alternatives and add-ons.*** The Administration's export controls are in no way preventing foreigners, let alone those with criminal intent, from obtaining access to encryption products. In fact, foreign software and hardware manufacturers have seized the opportunity to create sophisticated encryption products and to capture sales.

The General Accounting Office confirmed in 1995 that sophisticated encryption software was widely available to foreign users on foreign Internet sites. For example, Pretty Good Privacy ("PGP") – with 128-bit keys – is available for free on the Internet and is soaring in popularity.

A 1996 Department of Commerce study confirmed the widespread availability of foreign manufactured encryption programs and products, and an on-going industry study by Trusted Information Systems (TIS Study) reveals that as of December 1996, there were

570 foreign programs and products available from 28 countries, 229 of which employ DES.

Moreover, individuals may easily transmit U.S. developed programs overseas using a modem and the public telephone network without fear of detection. The TIS Study reports that there are 823 American programs and products – 378 with DES – readily transferable abroad over the phone lines.

If an encryption product is combined with other applications such as Internet browsers and servers, U.S. companies may lose both sales. One recent study estimates that by the year 2000, the computing industries' revenue losses due to U.S. export controls will be \$60 billion annually.

I would like to mention a few specific examples with respect to foreign availability of encryption products. The Apache Group, based in the U.K., announced last April that its Apache Unix Internet Server software with very strong encryption had a 29% market share. Today it is 43%.

At least six foreign companies (in Germany, Belgium, Switzerland, the U.K., Ireland, and Australia) have recognized the void for stronger encryption products and have responded to local customer demand for stronger encryption products by developing add-on products that easily allow anyone with a Web browser to download software off the Internet and thereby upgrade their "export-crippled" U.S. products from 40-bits to 128-bits. Moreover, in developing these add-on products they neither require nor depend upon any technical assistance from U.S. companies. To the contrary, they utilize standard programming techniques and free, public-domain versions of encryption algorithms and Internet security protocols to develop products that completely avoid U.S. export controls.

Other companies such as Brokat Informationssysteme, a German company, are developing products that are more than simply add-ons to American products. Brokat uses its strong cryptography as a means to sell more complicated software that will securely link a bank's conventional bank systems to its Internet gateways and online services. Brokat can count more than 30 banking and financial institutions located in the U.K., Switzerland and Germany as their customers. Brokat is now also exporting its products to the United States and trying to obtain U.S. export clearance to reexport a combination of their encryption product with a U.S. software product back overseas. (See Edmund L. Andrews, *U.S. Restrictions Give European Encryption a Boost*, N.Y. Times CyberTimes, April 7, 1997 and Peggy Salz-Trautman, *Brokat Eyes U.S. Software Rule*, Wall St. J. Interactive Ed., June 2, 1997)

***American companies are losing product sales every day because of current U.S. encryption export controls.*** Let me tell you about my company and one of our customers as an example.

The New Zealand Ministry of Health is building an Internet-based system for the management of personal medical data for the entire country. Because of the extreme

sensitivity of this data, they require 128-bit key encryption with no key recovery for communications. While they would like to purchase products from Sybase to build their system, they will not unless we can meet their security requirements. They have already identified two companies – R3 in Switzerland and Stronghold in the U.K – that they will turn to if U.S. export restrictions prevent them from getting the 128-bit security they require from Sybase.

A month ago, Sybase submitted an export application to the Department of Commerce for the New Zealand Ministry of Health. While we are hopeful that the application will be approved, there are three observations of particular importance to this Committee that I would like to make:

1. Unlike the current practice where all 40-bit encryption products are allowed to be exported after a one-time review, we need to apply for individual licenses each time we want to export a 128-bit encryption product. Even if our individual application is approved, the time and expense involved in acquiring individual export licenses is so high that this is not an economically viable approach for U.S. companies selling overseas.
1. Foreign competitors not subject to outdated U.S. export controls are ready to take sales and customers from U.S. companies today.
1. Current export controls do not keep strong encryption out of the hands of foreign customers; they just keep U.S. products out of their hands.

U.S. export controls have had the effect of creating an encryption expertise outside the United States that is gathering momentum. Thus, every time research and development of an encryption technique or product moves off-shore, U.S. law enforcement and national security agencies lose. Continuing down their present path will be more harmful to our national security and law enforcement efforts as American companies will no longer be the world leaders in creating and developing encryption products.

The NRC Committee concluded that as demand for products with encryption capabilities grows worldwide, foreign competition could emerge at levels significant enough to damage the present U.S. world leadership in information technology products. The Committee felt it was important to ensure the continued economic growth and leadership of key U.S. industries and businesses in an increasingly global economy, including American computer, software and communications companies. Correspondingly, the Committee called for an immediate and easy exportability of products meeting general

commercial requirements – currently the 56-bit DES level encryption. The Committee also noted that this would have to be updated periodically. It is now 16 months since the publication of this report, and a significant portion of Sybase customers are now demanding 128-bit encryption.

### **The Administration's Key Recovery Scheme and Other Similar Plans Are No Solution**

*The Administration's policy does not offer real export control relief.* The new regulations do not permit the easy exportability of 56-bit encryption products as called for by the NRC in its CRISIS Report. Instead they only permit the export of such products for up to 2 years if companies commit to produce or market "key escrow" or "key recovery" products that meet government – as opposed to market-based – requirements. Moreover, companies must submit a detailed business and marketing plan for government approval and pass a progress report every six months in order to be allowed to continue exporting 56-bit encryption products in the interim. (After two years, companies will be limited to servicing and supporting customers of already existing 56-bit products.) This requirement for 6-month renewable licenses subject to ongoing U.S. Government review is burdensome and intrusive and may serve as a disincentive to software vendors who might otherwise be interested in developing key recovery products.

The Administration's policy permits U.S. software and hardware manufacturers to export strong encryption only if their products provide the encryption key ("key escrow") or other decryption means ("key recovery") (1) in advance (2) to a government approved third party, (3) who could decrypt a user's stored data and communications if the Government so demands pursuant to court order. Unfortunately, the exportability of market-driven, commercially-motivated stored data recovery products remains very uncertain.

The regulations also generally ignore the realities of mass-market software distribution. Mass-market software publishers have invested hundreds of millions of dollars in developing multiple distribution channels such as OEMs (*i.e.*, hardware manufacturers that pre-load software onto computers), value-added resellers, retail stores and the emerging channel of on-line distribution. The mass-market distribution model presupposes that software publishers will take full advantage of these multiple channels to ship identical or substantially similar products worldwide (allowing only for differences resulting from localization) irrespective of specific customer location or characteristics. But the regulations require specific knowledge of customers to qualify them as key recovery agents and impose reporting and record keeping requirements that are ill-suited for mass-market products. Compliance with these requirements would be impossible without substantial changes in current methods of software distribution, as well as the collection of downstream information that is neither readily available nor of any obvious utility to enforcement officials.

*The Administration's key recovery scheme, and other similar plans, are too complex and too vulnerable. Technologically, it will not work, and users do not want it.* Let me

explain why. A huge bureaucracy will be necessary to manage the Administration's key recovery scheme. The Administration's proposal assumes that we can effectively accommodate the needs of dozens of governments, thousands of companies, tens of thousands of law enforcement offices, and millions of users. It also assumes that we can handle tens of millions of public-private key pairs and billions of recoverable session keys across thousands of different products. As the number of people using computers and the Internet grows, the number of keys that must be managed will explode. By the end of the decade, a key recovery system capable of accommodating all of the potential users around the world would have to be capable of handling many, many billions of keys. This is a very tall order. The bureaucracy to manage this key recovery system is likely to rival that of the Social Security Administration, the Internal Revenue Service, or the U.S. Postal Service.

The technology does not yet exist to create and smoothly operate a reliable system of this magnitude and complexity. Furthermore, the Administration's proposed key recovery scheme may actually make consumers more vulnerable. Advocates of a worldwide key recovery system conveniently overlook the tremendous technical barriers posed. It is unclear that such a system can be built at all, much less in the next few years. As Novell's CEO, Dr. Eric Schmidt stated, "Perhaps the technology necessary to create such a system will be available in my lifetime; it is not available today."

Cryptography experts report that "secure cryptographic systems are deceptively hard to design and build properly . . . Very small changes frequently introduce fatal security flaws . . . [A]dding key recovery makes it much more difficult to assure that such systems work as intended. It is possible, even likely, that lurking in any key recovery system are one or more design, implementation, or operational weaknesses that allow recovery of data by unauthorized parties." (See The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption, A Report By An Ad Hoc Group of Cryptographers and Computer Scientists, May 1997.)

Despite widespread claims of international agreements on "key recovery" infrastructures, no such agreements exist today. Bilateral and/or multilateral agreements must be negotiated and foreign governments' rights and responsibilities must be defined before the Administration's key recovery system can be created. Despite years of insisting that these treaties were just around the corner, the Administration has yet to conclude a single bilateral, much less multilateral, agreement with another government on key recovery. Nor has the Administration outlined any rights or responsibilities for foreign governments requesting access to U.S. decryption keys held by key recovery agents. It is not even clear whether these keys are subject to civil discovery in addition to criminal discovery.

Recently, ministers and business leaders from 30 European nations attending an Internet conference in Bonn, Germany, criticized the U.S. key recovery policy that requires guaranteed access for law enforcement. The ministers agreed in the Bonn Declaration that "they will work to achieve international availability and free choice of cryptography products and interoperable services, subject to applicable law, thus effectively

contributing to data security. If countries take measures in order to protect legitimate needs of lawful access, they should be proportionate and effective and respect applicable provisions relating to privacy." The German Economics Minister, Guenter Rexrodt, in fact opened the conference by calling for the removal of restrictions on encryption technology. (See *Should Encryption Software Have Limits?*, MSNBC Reuters Report and Jack Breibart, *Europeans Hit U.S. Encryption Policy*, American Reporter Correspondent.)

Criminals and terrorist groups will merely avoid using the Administration's key recovery scheme. The stated purpose of the Administration's key recovery scheme is to strengthen law enforcement and national security. But it is unlikely that criminals and terrorist groups will use a key recovery system that requires them to provide their keys to third-parties who can, in turn, give them to government officials. It is not clear that a global key recovery scheme can be designed so that it is impossible to circumvent, let alone with sufficient guarantee to make it impossible for criminals to avoid using it. Criminals have already shown that they can easily evade lawful wiretap and key escrow warrants and subpoenas by using a stolen or cloned cellular phone to connect to the Internet. There is no indication that they will not do the same when it comes to the Administration's key recovery scheme.

***S. 909 is also a significant step backwards.*** Unfortunately, other similar attempts at forcing key recovery are also fatally flawed. The Senate Commerce Committee recently adopted S. 909, the Secure Public Networks Act, which promotes the Administration's mandated third party key recovery access, and is a significant step backwards for American consumers. In fact, far from being a compromise, S. 909 is actually worse than the status quo. The bill sets up an extremely convoluted domestic key recovery system that is even more detailed than the one originally proposed by the Administration and requires the President to try and make it a worldwide system. This complex key recovery scheme will inevitably sacrifice business' and consumer's security and drastically increase their costs unnecessarily.

***The Administration's plan appears to differ significantly from the voluntary key recovery or data recovery functions for stored data desired by customers.*** There has been much discussion about obtaining access to the keys with which users encrypt information. For example, it is certainly possible to envision companies or organizations wanting access to the keys of their employees so as to be able to recover encrypted information generated in the course of their work. Several U.S. vendors offer commercial products that allow someone within the organization, or a third party voluntarily entrusted by that organization, to access the decryption key under defined policies. Individuals at home also might want the convenience and assurance of recovering their information in the event that they forget or lose their key.

But unlike government key escrow or key recovery proposals, the commercial demand for key recovery or data recovery encryption is limited to stored data (including e-mail, which is a "store and forward" product). It does not extend to real-time communications for several reasons:

- Users of commercial encryption applications have little reason to recover the "session" keys used to protect their communications. If a communication is successful, senders and receivers of encrypted communications already have access to plain text; if it is unsuccessful, the easiest and most obvious solution is simply to re-send the encrypted communications using a new "session" key.
- A number of popular Internet protocols generate new session keys **each and every time** a user connects to a Web site or communicates in any way over the Internet. Thus, hundreds of millions of Internet and intranet users will create hundreds of billions of session keys, and these numbers will grow by orders of magnitude as the expected communication revolution pushes more people online.
- Developing and maintaining a key management infrastructure for storing and retrieving this vast number of communication session keys adds cost and complexity to encryption systems, and primarily benefits law enforcement agencies engaged in surveillance activities.

Furthermore, permitting a user to recover data is not the same as forcing them to provide a key or other decryption means to a third party who must be approved by the U.S. Government.

In addition, the Administration's new regulations are too tenuous for many software companies to invest in developing mass-market encryption products that meet the requirements of the Administration's plan. It also is unclear how the plan would work for millions of small and medium-size businesses or individuals who may lack the expertise and resources of large corporations and government agencies. Companies are unlikely to develop products if they are unsure that they will be purchased and would be approved for export.

I would note that for all these reasons, the NRC Committee recommended a policy of "deliberate exploration" for key escrow and key recovery, rather than one of "aggressive promotion." We could not agree more.

In order for any encryption policy to succeed, it must be market-driven. It must be flexible and recognize that encryption is used by individuals in a wide variety of settings and for a broad range of purposes (*e.g.*, user authentication and integrity checks, stored data, financial applications, communications).

Importantly, to the extent that key recovery or data recovery encryption products are widely used, then much information will be available to the government for law enforcement purposes under appropriate judicial procedures – just like physical property, including memoranda, letters, and files, is today. But users must see the value of key recovery features and want to use them. Whereas if the government mandates undesirable

encryption products, the likely result is that no one will use products implementing these features thereby frustrating law enforcement objectives. In short, any key recovery system must result from a user-driven, market-led process. It cannot be a mandated, government-designed, top-down, one-size-fits-all, complicated solution.

*Ultimately, the Administration's policy is an attempt to use export policy to control the domestic use of encryption.* As the Congressional Research Service recently stated, "[u]sing the export process to restrain the availability of strong encryption remains a core principle of Clinton Administration policy." There can be little doubt about the real thrust of the Administration's policy; indeed, in 15 pages of detailed Federal Register text, there is only one sentence that addresses who can be an acceptable foreign key agent – presumably of great interest to foreign users!

The domestic software industry makes approximately one-half of its revenues through exports, and customers are increasingly demanding uniform encryption capabilities. Therefore, most mass-market software and hardware is designed to offer the same encryption capabilities both domestically and abroad. Thus, this new policy effectively forces domestic encryption hardware and software into the Hobson's choice of maintaining separate product lines for the domestic and international markets or complying with the Administration's export restrictions. Moreover, the FBI has said it is willing to seek legislation mandating domestic encryption restrictions if the effort to leverage export controls fails.

### **BSA Strongly Supports the SAFE Act Because It Provides**

#### **Needed Export Control Relief**

The SAFE Act recognizes as a fundamental proposition that the United States should not try to control the export of something that is, by its very nature, uncontrollable. It makes little sense for our government to require individual export licenses for the export of mass-market software when it is generally available to the public in retail outlets, pre-loaded on computers, over the Internet, and in the public domain. Nor should computer hardware be so controlled simply because it incorporates such software. In short, it makes little sense to continue trying to control exports of software that is already available to millions of people both domestically and abroad. Nothing inherent about encryption software alters this conclusion: it is still software and still easily and readily available on a worldwide basis.

Importantly, the SAFE Act does permit the Secretary of Commerce to continue preventing exports to countries of terrorist concern or other embargoed countries pursuant to the Trading With The Enemy Act or the International Emergency Economic Powers Act.

The SAFE Act ensures that if strong encryption products have been permitted to be exported to foreign banks, then they should be exportable to other foreign commercial purchasers in that country. Note that the type of software and hardware we are talking

about here is a "custom" product (if it were generally available it would not need an individual license under the bill's other provisions). Because it is at least theoretically possible to control such exports, the question then occurs as to what should be the allowable level of encryption.

Once again, the bills do contain safeguards when relaxing export controls for such products – the Secretary of Commerce is not required to permit such exports if there is substantial evidence that the software will be diverted or modified for military or terrorist use or re-exported without requisite U.S. authorization.

I also want to note that we believe the sponsors and supporters of the SAFE Act have made a wise decision in seeking to make explicit what is now implicit under existing laws – that there is not and should not be any restriction on the domestic use, choice or sale of strong cryptography. Some argue that it is already law because there is nothing to the contrary. That is correct; nevertheless, we believe that it is important and helpful to explicitly reaffirm the rights of Americans in this area.

The time for action is now. To keep American vendors on a level international playing field and American computer users adequately protected, U.S. export controls must be immediately updated to reflect technological and international market realities.

Thank you.