

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

**INTERNATIONAL ECONOMIC POLICY AND TRADE
SUBCOMMITTEE of the**

INTERNATIONAL RELATIONS COMMITTEE

U.S. HOUSE OF REPRESENTATIVES

Washington, D.C.

May 8, 1997

Good Morning. My name is Thomas Parenty and I am the Director of Data and Communication Security for Sybase, Inc. 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 and mid-eighties. While at the NSA, I worked on the security of global nuclear command and control networks, focusing on the formal verification of cryptographic protocols and internal computer access controls. In addition, I advised the Director of the NSA (DIRNSA) on internal NSA computer security issues. Additionally, 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 and the Air Force as well as many U. S. computer vendors.

Headquartered in Emeryville, CA, Sybase, Inc. 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 the Business Software Alliance ("BSA") which represents the leading U.S. software companies Adobe, Apple Computer, Autodesk, Bentley Systems, Compaq, Lotus Development, Microsoft, Novell, The Santa Cruz Operation, Symantec, and my company, Sybase.

Companies such as Sybase, and the American software industry, as a whole 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. Therefore, I am really here today to speak on behalf of the tens of millions of users of American software products.

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, such as Sybase have innovative products that can meet this demand and compete internationally. However there has been one impenetrable obstacle – the application of overbroad, unilateral, export controls by the U.S. Government.

For that reason BSA strongly supports H.R. 695, the Security and Freedom through Encryption (SAFE) Act. If passed, H.R. 695, along with its counterparts in the Senate S. 377 and S. 376, ProCODE and ECPA respectively, would permit American software companies to compete on a level international playing field and to provide computer users with their choice of protection for their confidential information.

The Importance Of The American Software Industry

Today, computer users – our customers – enjoy unprecedented access to information that is changing the way we all live and work. This is true whether users are in the largest of cities or the most isolated of rural communities. Importantly, the Internet, which is driving the current "Information Age," is made possible by software that routes data and helps users navigate oceans of information. Fortunately, to this point, the U.S. computer software industry has been the world leader.

Indeed, the incredibly dynamic U.S. computer software industry is an American success story. Since 1980 the industry has grown seven times faster than the rest of the economy and today is now larger than all but five manufacturing industries. Conservative estimates are that more than 1.2 million people are employed in the software, hardware and semiconductor industries – with more than 500,000 people in the computer software industry alone. This economic success has fueled research and development for new generations of products and spurred the creation of numerous market-leading products and choices.

The computer software industry is one of our country's most internationally competitive. American-produced software accounts for over 70% of the world market in software, with exports of U.S. software programs constituting half of many software companies' revenues. 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.

The Need For Immediate Export Control Relief

1. The Importance Of Encryption

Strong encryption becomes critical to secure information in today's networked world. Millions of personal computers are connected through private networks and the public Internet. 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.

Strong encryption is essential to protect the confidentiality and privacy of sensitive personal and confidential business electronic information, as well as ensure its authenticity and integrity. Without encryption, businesses and individuals will not entrust their valuable proprietary information, creative content, and sensitive personal information to electronic networks and risk unauthorized disclosure, theft or alteration of their information or transaction. The promise and potential of the Internet simply will not materialize. Companies will hesitate to design new products or work collaboratively from remote sites. A routine visit to the doctor becomes an invasive procedure unless your records can be kept private. Electronic banking and commerce, a demand of many computer users, will not happen "on-line" without strong encryption.

The widespread use of encryption is also necessary to protect our national and economic security. Without encryption, the electronic networks that control such critical functions as airline flights, health care functions, electrical power and financial markets remain highly vulnerable. Indeed, 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; that such attacks are costly and damaging; and that such attacks on Defense and other U.S. computer systems pose a serious threat to national security.

For all these reasons, computer users worldwide are demanding stronger encryption to protect the security and privacy of their electronic information. American computer software and hardware companies have responded by developing programs and products with strong encryption.

2. The Problem With Current Unilateral U.S. Export Controls

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 and they cannot use those same programs overseas. This is problematic for users because they need global interoperability and for software companies because of the marketing difficulties in selling foreign purchasers a less strong version of an encryption product as well as the additional cost of developing and selling two versions of a program worldwide.

Until very recently, 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 in exchange for proof of commitments to build key recovery into future products. However, these licenses are not easy to get and 40-bits remains the level for which easy export is still permitted. This policy ignores the fact that:

- The current world benchmark is at least DES with 56-bit keys, with 112 and 128-bit keys increasingly being used;
- 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.
- Hundreds of alternatives are available from foreign manufacturers and off the Internet (about half using DES or stronger encryption); and
- 40 bit encryption is increasingly vulnerable to commercial attack.

Ironically, the people most harmed by the Administration's export controls are American companies and American computer users – a perfect example of "the tail wagging the dog." Because exports account for over one-half of the American software industry's revenues, U.S. software companies mostly focus their efforts on software that can be shipped both domestically and abroad. The effect of the Administration's policy is thus to limit the effectiveness, variety and availability of encryption products in the United States.

American companies face strong competitive disadvantages overseas and are losing product sales every day because of current encryption export controls. For example, a Sybase customer, a large Wall Street firm, is unable to offer services and products overseas because current export regulations do not permit adequate protection for sensitive personal information. The customer loses money because it can't sell products and services overseas, and Sybase loses because we can't sell the customer the products that it would need if they could sell overseas.

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. Thus, the Administration's policy is harming the U.S. industry's international competitiveness. America's software companies should not be forced to play catch-up in a market which they currently dominate with a 70 percent worldwide market share.

In short, the inability of American software and hardware companies to supply their users with strong encryption to meet their legitimate needs for information security directly threatens the continued success of our industry. Moreover, it means American computer users' electronic information remains vulnerable. Finally, and perhaps most importantly, U.S. export controls threaten to dislodge continued American leadership in developing the Internet.

A. The Current World Benchmark Is At Least DES With 56-Bit Keys, With 112 And 128-Bit Keys Increasingly Being Used

The Data Encryption Standard (DES) algorithm with 56-bit key lengths was developed by government and industry in the 1970's. It remains the U.S. Government's standard for unclassified confidential information (although appears to be wearing thin). Thus, all the proposed "Internet Protocols" addressing security call for encryption at least at the 56-bit DES level, recognizing the growing popularity of "triple DES" with 112-bit keys, as well as PGP and RC4 (used in virtually all Internet browsers), with 128-bit keys.

It is essential to understand that the backbone of the Global Information Infrastructure is the Internet – a network of networks not controlled by any one government or organization. In the last few years, American companies have recognized that they must adapt their business plans to work with the Internet, rather than instead of, or even in addition to, the Internet. Companies wishing to provide software for, or do business on, the Internet must acknowledge such standards if they are to have any chance of gaining widespread acceptance.

B. Continued Unilateral U.S. Export Controls Have Not Been Effective in Restricting The Availability of Foreign Encryption Products

Continued unilateral U.S. export controls have not been effective in restricting the availability of encryption abroad. Foreign software and hardware manufacturers have seized the opportunity to create sophisticated encryption products and to capture sales. A 1996 Department of Commerce study confirmed the widespread availability of foreign manufactured encryption programs and products, and an on-going industry study reveals that as of January 1996, there were 570 foreign programs and products available from 28

countries, 229 of which employ DES. (There are also 823 American programs and products – 378 with DES – readily transferable abroad with a modem and public telephone line).

I would like to mention just two specific examples with respect to foreign availability of encryption products. First, 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%. BSA has learned that approximately six foreign companies (in Germany, Belgium, Switzerland, the U.K., Ireland, and Australia) have recognized the void for stronger encryption products. The companies 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. Is any clearer evidence needed that the genie is out of the bottle?

The General Accounting Office also 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. Moreover, individuals may easily transmit U.S. developed programs overseas using a modem and the public telephone network without fear of detection. Clearly, the Administration's export controls are in no way preventing foreigners, let alone those with criminal intent, from obtaining access to encryption products.

3. The NRC's CRISIS Report Echoes These Views

As you probably know, a blue ribbon National Research Council (NRC) Committee has called for U.S. policies which foster the broad use of encryption technologies in its May 1996 CRISIS Report ("Cryptography's Role in Securing the Information Society"). The Committee's report echoes what industry has been saying for several years regarding the need for export control relief. Importantly, the 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.

The Administration's "New" Policy Does Not Solve the Problem

On October 1, 1996, the Administration announced a new encryption policy claiming that it would let industry take the lead in developing a worldwide key management infrastructure and purporting to make it easier to export 56-bit encryption products. This had been the strong recommendation of an expert National Research Council Committee (after a two year study) and many in the private sector hoped that the Administration had decided to follow that advice.

On November 15, 1996, the Administration transferred all commercial encryption items from the U.S. Munitions List to the Commerce Control List. However, while this should result in easy exporting, the Administration appears to be continuing to impose many of the same stringent national security and foreign policy controls traditionally applied to munitions. Thus the provisions of the commercial export control regulations which permit products to be exported when they are available from foreign sources or publicly available are deemed inapplicable for encryption items. In short, the forum changed, but not the substance!

On December 30, 1996, the Department of Commerce's Bureau of Export Administration issued new detailed Export Administration Regulations ("EAR") to further implement the Administration's policy. Unfortunately, the regulations do not appear to deliver on the Administration's earlier promises. They do not offer easy export of 56-bit encryption products as products as called for by the National Research Council in its May 1996 CRISIS Report. According to the regulation, products will only be permitted for export for up to 2 years if companies commit to produce or market future government acceptable "key escrow" or "key recovery" products. 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, with no cost of cracking adjustment for the inevitable increase in technology during the interim.) There is no predictability in such a system. No ability for customers and software producers to plan.

According to these regulations, the Administration's policy is to permit 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. The exportability of market-driven, commercially-motivated stored data recovery products not meeting this requirement remains very uncertain.

The Administration's policy is an attempt to use export policy to control the domestic use of encryption. As CRS 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! As I explained earlier, 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 appears to force domestic encryption hardware and software to comply with the Administration's export restrictions. Moreover, the FBI has said it is willing to mandate *domestic* encryption restrictions if the effort to leverage export controls fails!

In further analysis of the Administration's policy, Sybase has applied for an export license for several mass market software products with encryption capabilities. In our application, we outlined an approach to key recovery, which is based on customer need, technical feasibility, and market acceptance. Even if licenses are granted for such products, it is on a case by case basis which could lead to picking winners and losers in the marketplace. Therefore, legislation is needed to establish a consistent policy for granting export licenses.

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. Presumably someone within the organization, or a third party voluntarily entrusted by that organization, would be able to access the decryption key. Individuals at home also might want the convenience and assurance that they will be able to recover 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 store and send). It does not extend to real-time communications which could just as easily be resent.

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 of our companies to decide to develop mass market encryption products. The so-called "key management infrastructure" envisioned by the Administration is not in place. It also is unclear how it would work for millions of individuals who are not in large corporations or governmental entities. 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 couldn't 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.

BSA Strongly Supports Pending Legislation Because It Provides

Needed Export Control Relief

The SAFE, Pro-CODE and ECPA bills recognize that it makes little sense for our government to require individual export licenses for the export of software that is generally available by virtue of being mass marketed commercially, distributed via the Internet, or found in the public domain. Nor should computer hardware be so controlled simply because it incorporates such software. In short, if it is "out there," if it is already available to millions of people easily and readily transferable electronically, then it makes little sense to continue trying to control such exports.

Importantly, the bills do 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.

Finally, I do want to note that we believe the sponsors and supporters of the various bills 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.

Conclusion

The inability of American software and hardware companies to supply their users with strong encryption to meet their legitimate needs for information security directly threatens the continued success of our industry. It means American computer users' electronic information remains vulnerable. U.S. export controls also threaten to dislodge continued American leadership in developing the Internet.

One last and very important point. The NRC Report found, 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 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."

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

Thank you.