

**Testimony Of**

**THOMAS PARENTY**

**DIRECTOR, DATA/COMMUNICATIONS SECURITY**

**SYBASE, INC.**

**On Behalf Of The**

**BUSINESS SOFTWARE ALLIANCE**

**PROTECTING PUBLIC AND PRIVATE NETWORKS  
THROUGH U.S. SOFTWARE WITH ENCRYPTION CAPABILITIES  
IS CRITICAL TO AMERICA'S NATIONAL SECURITY**

**Before The**  
**NATIONAL SECURITY COMMITTEE**  
**U.S. HOUSE OF REPRESENTATIVES**  
**Washington, D.C.**

**July 30, 1997**

**Introduction**

Good Morning. My name is Thomas Parenty, and I am the Director of Data and Communication 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 and 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.

Today, I am here to make three critical points:

First, the tens of millions of users of American software products are demanding strong security worldwide.

Second, encryption is necessary to ensure America's national and economic security because it prevents crime on computer networks. Furthermore, the continued success of the U.S. software and hardware industries in the worldwide market for products with encryption capabilities is also critical to America's national and economic security.

Third, the Administration's key recovery scheme, and other similar plans, are inherently imperfect and, if mandated, will likely cause an increase in crime.

For these reasons, BSA thanks the members of the Committee who have cosponsored H.R. 695, the Security and Freedom through Encryption (SAFE) Act, which has over a majority of the full House of Representatives as cosponsors (approximately 250 and growing). BSA also urges the Committee to report the SAFE Act principally unamended as it was reported by both the House Judiciary and International Relations Committees.

### **Users Are Demanding Security 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. 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.

The U.S. Government recognizes many of the threats in the new digital world. In fact, FBI Director Freeh recently testified in one of the FBI's proposed initiatives for the 1998 budget that "[i]llegal electronic intrusion into computer networks is a rapidly escalating crime problem. White collar criminals, economic espionage agents, organized crime groups, foreign intelligence agents, and terrorist groups have been identified as 'electronic intruders' responsible for penetrations of American computer networks. It is estimated that the Pentagon's computers are subject to hackers' attempts 250,000 times a year."

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.

### **Encryption Is Necessary to Ensure America's National and Economic Security.**

Strong, secure encryption does not just aid criminals, it prevents crime. It is obvious that encryption can be used by criminals. From rum-runners of old to drug-cartels of the present, criminals often are very clever in concealing their activities, and PCs and the Internet have become tools of their trade, alongside telephones, facsimile machines, and pagers. As you also know, virtually every major business and government worldwide now runs on – in fact now depends upon – computer networks that communicate with other computer networks. Strategic information flows through these networks, and all of their critical systems depend upon the integrity of these networks.

In this age of computer networks and widely dispersed information flow, corporations are demanding strong, secure information systems. Similar to the government, corporations "compartmentalize" their critical business information, and strictly control access to these compartments. Not everyone is trustworthy within a company, and it is this security, this compartmentalization, that prevents crimes such as insider trading, leakage of trade secrets, and corporate espionage.

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. We will see many, many hundreds of millions in losses, and we may possibly see the destabilization of a company, the stock market or perhaps even a whole economy.

Thus, information security is critical to the integrity, stability and health of both 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 56-bit DES as a minimum, and much larger key-length, stronger encryption for financial applications as well as many other applications such as enterprise-wide messaging systems.

Correspondingly, widespread use of encryption is also necessary to protect America's 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;
- Such attacks are costly and damaging; and
- Such attacks on Defense and other U.S. computer systems pose a serious threat to national security.

The interests of computer users, hardware and software companies and privacy groups, therefore, 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."

### **Continued Success of the U.S. Software and Hardware Companies in the Worldwide Market for Products with Encryption Capabilities Is Critical to America's National and Economic Security**

*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. 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.

***Unilateral U.S. export controls are not stopping the use or development of encryption products. Instead, the result is that encryption expertise is being developed off-shore by foreign companies.*** 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.

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, the Administration wants to define "key recovery" in its own terms, not in consumer-driven

terms, and the licenses are not easy to get. Therein, 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.

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. 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. In fact, 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 by Trusted Information Systems reveals that as of December 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). 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. 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%.

There are approximately six foreign companies (in Germany, Belgium, Switzerland, the U.K., Ireland, and Australia) which 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)

Correspondingly, 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 cannot sell products and services overseas, and Sybase loses because we cannot sell the customer the products it would need to sell such products and services overseas.

In fact, just this past week, I was speaking with another Sybase customer, the New Zealand Ministry of Health, who 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 have the requirement to use 128-bit keys without key recovery. 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 security they require from Sybase.

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 threatens national security and domestic law enforcement. Without widespread use of strong encryption, networking systems are insecure, providing opportunities for hackers, common thieves and terrorists.

***Continued access by the U.S. Government to U.S. cryptographers' expertise and U.S. companies' encryption products is critical to America's national security.*** When called upon with the appropriate legal measures, American cryptographers and American companies have responded to requests by the U.S. Government for information regarding encryption. They are willing to help keep law enforcement and national security agencies abreast of emerging technologies so that the U.S. Government will be able to execute effectively its responsibilities.

Additionally, American companies must file for export approval for strong encryption with the Bureau of Export Administration at the Department of Commerce. At this time, the U.S. Government has an opportunity to ask questions and evaluate the encryption component included in U.S. software and hardware products. Thus, whether an export license is needed or not, American companies provide important information to the government. The U.S. software and hardware industries' success in the worldwide marketplace today provides America's law enforcement and national security agencies with advantages they will not have if the market is ceded to foreign software developers.

Furthermore, 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 loose. 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's CRISIS Report.*** As you probably know, the NRC Committee in its CRISIS Report called for U.S. policies which foster the broad use of encryption technologies. 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 Key Recovery Scheme, and Other Similar Plans Are Inherently Imperfect and, if Mandated, Could Lead to an Increase in Crime**

My message is simple — **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 Breitbart, *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.

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 a key recovery scheme will inevitably sacrifice business and consumer's security and drastically increase their costs unnecessarily.

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

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

SAFE recognizes 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. By ensuring a level playing field with foreign companies, SAFE will enhance U.S. national security and law enforcement efforts by ensuring secure public networks and allowing American companies to maintain their worldwide lead in the software market. 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.

The time for action is now. U.S. export controls must be immediately updated to reflect technological and international market realities.