PREPARED STATEMENT OF IRA RUBINSTEIN,
SENIOR CORPORATE ATTORNEY, MICROSOFT CORP.,
ON BEHALF OF THE BUSINESS SOFTWARE ALLIANCE

Security and Freedom Through Encryption (SAFE) Act
March 20, 1997 - House Judiciary Subcommittee on Courts and Intellectual Property

Good Morning. My name is Ira Rubinstein, and I am a Senior Corporate Attorney with Microsoft Corporation at its headquarters in Redmond, Washington. Over the past twenty years, Microsoft has sought to empower personal computer users by developing software that makes it easier for them to use their PCS at home and at work for an increasing number of purposes. In pursuit of this goal, Microsoft has grown, changed, adapted and reinvented itself continuously today we employ nearly 19,000 people, approximately 9,000 of which are located at our headquarters in Redmond, Washington. We are now one of the leading software publishers with products ranging from operating systems, to applications software such as word processing and spreadsheet programs, to software development tools and programming language products that help people develop and write creative software, and to an Internet on-line service, the Microsoft Network (''MSN'').

I greatly appreciate the opportunity to appear today before this Committee on behalf of the Business Software Alliance (''BSA''). The Business Software Alliance 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 Computer Associates, Compaq and 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 communicate securely worldwide. American companies have innovative products that can meet this demand and compete internationally. But there is one thing in our way the continued application of overly broad, 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. Right at the start I want to commend Representative Goodlatte for his vision and leadership in introducing this bill. I want to thank you, Chairman Coble, for your support and willingness to hold a hearing on this bill so quickly. I also want to recognize the other members of this Subcommittee who have cosponsored the bill—Representatives Conyers, Sensenbrenner, Bono, Pease, Cannon, Boucher, and Lofgren. You also have been joined in cosponsoring the bill by a number of other members of the Judiciary Committee—Representatives Gekas, Smith, Inglis, Bryant, Chabot, Barr, Jackson Lee and Waters. Although hearings in both the House and the Senate occurred last year, there was insufficient time to move the legislation forward. By starting early this year, we are hopeful that legislation will be enacted in the very near future. Certainly, the 61 total co-sponsors to date is indicative of broad bi-partisan support.

I also want to thank Senator Burns for introducing S. 377, the Promotion of Commerce On–Line In The Digital Era (Pro-CODE) Act, and Senator Leahy for introducing S. 376, the Encryption Communications Privacy Act (ECPA).

While these bills differ in some respects, they *all* modernize export laws regarding software and hardware with encryption capabilities to permit American software companies to compete on a level international playing field and to provide computer users with their choice of adequate 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 Global Information Infrastructure, which is driving the current ''Information Age,'' is made possible by software that routes data and helps users navigate oceans of information. Fortunately, to date, 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 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 and spurred the creation of numerous market-leading products.

The computer software industry is one of our country's most internationally competitive. American-produced software accounts for over 70 percent 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 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 in a networked world. Today, millions of personal computers are connected through private LANs and WANs and the public Internet. Companies, governments and individuals are now realizing that they can no longer protect data and communications from intruders by relying on securing physical access to computers or relying on 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 transactions. The promise and potential of the Global Information Infrastructure simply will not materialize. Companies will hesitate to design new products or work collaboratively from remote locations. A routine visit to the doctor becomes an invasive procedure unless your records can be kept private. Electronic banking and commerce 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 features.

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 which 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 international customers because they need global interoperability; and it is problematic for U.S. software companies because foreign customers refuse to purchase weaker versions of an encryption product and it is very costly to develop, market and distribute two versions of a program worldwide.

American software companies have been unable to upgrade the strength of their encryption beyond the 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. This 40-bit level ignores the facts that:

I. The current world benchmark is at least DES (56-bit keys) and triple-DES (112-bit keys) and 128-bit key RC4 are increasingly common;

II. Hundreds of alternatives are available from foreign manufacturers and off the Internet (about half using DES or stronger encryption); and

III. 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 which 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.

Also, American companies face a strong competitive disadvantage overseas and are losing encryption product sales. 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 not only the Global Information Infrastructure, but the next generation of security technology.

A. The Current World Benchmark Is At Least 56-Bit DES, With Triple-DES and 128-Bit RC4 Increasingly Common

The Data Encryption Standard (DES) algorithm with 56-bit key lengths was developed by government and industry in the 1970s. It remains the U.S. Government's standard for unclassified confidential information (although it appears to be wearing thin). Thus, all the proposed ''Internet Protocols'' addressing security call for encryption at least at the 56-bit DES level and recognize the growing popular demand for ''triple DES'' (112-bit keys) and the RC4 algorithm 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 their products or services 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. An on-going industry study reveals that as of January 1996, there were 497 foreign programs and products available from 28 countries, 193 of which employ DES. (There are also 684 American programs and products—330 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 UNIX-based Apache Server is the number-one Internet server product, with a 43 percent market share, up from 29 percent market last April. Stronghold, a U.K. company, markets a secure version of Apache that incorporates a protocol for secure communications at 128-bits. Second, we have identified at least one-half dozen foreign software companies (in Germany, Belgium, Switzerland, the U.K., Ireland, and Australia) who 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. These vendors have recognized the void created in Internet security products by U.S. export controls and have responded accordingly. 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 avoids 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 Internet sites hosted outside the U.S.. 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.

C. 40-bit Encryption Is Increasingly Vulnerable To Commercial Attack

Finally, we believe that there can be little dispute that information encrypted at the 40-bit level no longer provides sufficient protection against even casual hackers using idle computers. Students with Ecole Polytechnique in France and at our own MIT have successfully performed ''brute force'' attacks on 40-bit encryption. Also, more recently at the RSA encryption conference held in January, a student from University of California at Berkeley responded to RSA's challenge and decrypted a 40-bit encrypted message in only 3 1/2 hours. Indeed, a report released last year by seven leading private sector cryptologists and computer scientists highlighted the vulnerability of 40-bit keys to commercial attack.

3. The NRC's CRISIS Report Echoes These Views

As you know, in its May 1996 CRISIS Report (''Cryptography's Role in Securing the Information Society''), the blue ribbon National Research Council (NRC) Committee called for U.S. policies which foster the broad use of encryption technologies. 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. Therefore, the Committee called for an immediate and easy export ability 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 IS NO SOLUTION

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 listed on the State Department's U.S. Munitions List to the Commerce Department's Commerce Control List. However, while this transfer of jurisdiction should have resulted in easier exporting, the Administration continued to impose many of the same stringent national security and foreign policy controls traditionally applied to munitions! For example, the provisions minimizing export controls when U.S. companies demonstrate the availability of similar products from foreign sources, or the publicly availability of such products, 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 an interim rule amending the Export Administration Regulations (''EAR'') to further implement the Administration's policy. Unfortunately, the result fails to deliver on the Administration's earlier promises. The regulations do not offer easy export of 56-bit encryption products. Moreover, the regulations offer no assurances that a variety of market-driven, commercially-developed, voluntary ''key recovery'' or ''data recovery'' products using longer key lengths can be exported.

The Administration's policy does not offer easy export control relief. The new regulations do not permit the easy export ability of 56-bit encryption products as called for by the National Research Council in its May 1996 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 existing 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 export ability 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 in order 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 policy is flawed and ultimately self-defeating. 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 in order 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 the communications is

successful, senders and receivers of encrypted communications already have access to plaintext; 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 of our 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 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.

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! 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 forces domestic encryption hardware and software into the Hobson's choice of maintaining separate products 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.

The Administration's new policy will soon be tested. Finally, we wanted to take the opportunity to inform you that two weeks ago a BSA member company, Sybase, submitted an export application for a software product which encrypts both stored data and electronic communications. A user of this product may choose to permit one or more user-selected (and not necessarily government approved) third parties to have access to the keys used for encrypting stored data (but there is no such feature for communications).

The December 30th regulations state that the Administration may approve the export of ''recoverable encryption'' products which allow government access to unencrypted data and communications pursuant to court authorization without the knowledge of the user. However, the regulations provide no guidance or guarantees for exporting such products. Hence the need for a ''test case'' to determine whether the Administration will approve exports of market-driven encryption products for

which there *is* identified commercial demand. We look forward to determining whether this type of ''recoverable encryption'' product will be exportable under License Exception pageKMI.

BSA STRONGLY SUPPORTS PENDING LEGISLATION BECAUSE IT PROVIDES NEEDED EXPORT CONTROL RELIEF

The SAFE, Pro-CODE and ECPA bills recognize 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, and nothing about encryption software alters this conclusion: it is still software and still easily and readily available on a worldwide basis.

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 bills provide 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 bills 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.

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

U.S. export controls prevent American software and hardware companies from supplying their customers with strong encryption to meet their legitimate needs for information security and thereby directly threaten the continued success of our industry. Moreover, because U.S. vendors invest more heavily in developing products for worldwide markets, export controls also delay the introduction of sophisticated security products in the U.S. market, leaving American computer users electronic information vulnerable to hackers and other intruders. U.S. export controls also threaten to dislodge continued American leadership in developing the Global Information Infrastructure.

One last and very important point. 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 NRC Committee 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.