NOTE: ATTACHMENTS 1 THROUGH 3 ARE NOT INCLUDED IN THIS DOCUMENT

TESTIMONY

BY

STEPHEN T. WALKER
PRESIDENT
TRUSTED INFORMATION SYSTEMS, INC.

FOR

SUBCOMMITTEE ON ECONOMIC POLICY, TRADE AND ENVIRONMENT
COMMITTEE ON FOREIGN AFFAIRS
U.S. HOUSE OF REPRESENTATIVES

OCTOBER 12, 1993

Good Afternoon. I am pleased to testify today about the negative impact that U.S. export control regulations on cryptography are having on one of the few industries where the U.S. remains dominant worldwide: the information system software industry. The major points of my testimony are that U.S. export controls do not prevent the international availability of good quality cryptography but do penalize the U.S. software industry and U.S. business in general.

My name is Stephen T. Walker. I am the founder and President of Trusted Information Systems (TIS), Inc., a ten year old firm with 85 employees. With offices in Glenwood, MD; Los Angeles, CA; Mountain View, CA; Minneapolis, MN; and London, UK, TIS specializes in research, product development, and consulting in the fields of computer and communications security. I am also here representing the Software Publishers Association (SPA) and its members on this most important topic.

The SPA is the principal trade association of the personal computer software industry. Since 1984, it has grown to over 1,000 members, representing the leading publishers in the business, consumer, and education software markets.

My background includes twenty-two years as an employee of the Department of Defense, with the National Security Agency (NSA), the Defense Advanced Research Projects Agency, and the Office of the Secretary of Defense. During my final three years in Government, I was the Director of Information Systems for the Assistant Secretary of Defense for Communications, Command, Control, and Intelligence (C3I).

In 1983, I left Government service and began my own consulting firm, specializing in the area of information systems security. My company has experienced steady growth and now offers a variety of products with improved information security for military and civilian applications in addition to our continuing consulting activities. Several of these products are adversely affected by U.S. Government export controls, as are the products of many SPA members.

For the past two years, I have been a member of the Computer System Security and Privacy Advisory Board (CSSPAB), chartered by Congress in the Computer Security Act of 1987 to advise the Executive and Legislative Branches on matters of national concern in computer security. In March 1992, the Board first called for a national review of the balance between the interests of law enforcement/national security and those of the public regarding use of cryptography in the United States. The Board has been heavily involved in this review, receiving public input on the Administration's Clipper Initiative, announced by the President on April 16 of this year. Participation in the Board's review has been highly beneficial in helping me form my opinions in this area.

OVERVIEW

The focus of attention at today's hearing is the negative impact that U.S. export controls on cryptography are having on the U.S. computer industry. In May 1992, I testified before the House Judiciary Committee, Subcommittee on Economic and Commercial Law hearings, on the impact of U.S. export laws on our industry's ability to protect itself from foreign industrial espionage. I also participated in similar hearings in July 1991 and June 1990 in which this topic was of major importance. The export control subject continues to arise in different contexts, but the difficult problems lurking behind it are always the same.

The stakes for the software industry are high. The U.S. holds 75% of the global market for packaged software. Most software companies make 35-40% of their revenue from exports; for some companies exports are as much as 50% of their business. When demand for cryptographic products is increasing, export restrictions essentially place an "earnings cap" on U.S. software publishers.

A National Dilemma

The basic issue is a dilemma of truly national proportions between the long standing and vital interests of our Government to learn as much as it can about its adversaries--be they criminals, terrorists, or other governments--on the one hand, and the basic right to privacy that all Americans assume they have and are seeking to extend to their personal and business communications, whether by telephone, electronic mail, or other forms of computer communications.

The resolution of this dilemma will have enormous impact on our country for decades to come. The Government's national security interests contend that if good quality cryptography were to become widely available in this country and the world, our ability to wiretap criminals and listen in to terrorists and other adversaries would be severely hurt. Those seeking improved privacy protection argue that encryption is needed to support worldwide business operations and good quality cryptography is already available worldwide. Continuing U.S. Government restrictions are only penalizing U.S. users with inferior U.S.-developed security products and limiting U.S. industry from participating in a rapidly growing international marketplace.

Technology Has Shifted

The core of the issue is a shift in technology over the past twenty years that has fundamentally altered both business communications needs and an advantage that law enforcement and national security interests have enjoyed since the earliest days of electronic communications. Before radio and telephone communications, governments had to resort to intercepting mail and notes carried by spies to learn their adversaries' plans. When electronic communications became prevalent, governments found they could intercept those communications relatively easily with very useful results. When encryption was applied to these communications, it became more difficult to make sense of them, but that turned into a test of wits among the mathematicians of various countries. Some were more successful than others.

During the time up to the 1980s, this behind-the-scenes struggle was waged among governments with little if any effect on individuals or business communities. But technology shifts beginning in the early 1980s and accelerating at breathtaking rates today resulted in vast computer communications and security capabilities for industrial and personal use worldwide and at the same time have made it much harder for law enforcement and national security interests to continue their interception roles.

As we struggle to understand the complex issues confronting us in this dilemma, we must recognize that even if U.S. commercial and private interests were willing to forgo their right to private communications and U.S. computer manufacturers were willing to drop out of the international market for information products employing good quality security protection, the ability of the Government to decrypt the communications of its adversaries will continue to diminish at ever increasing rates over the foreseeable future, no matter what measures, such as employing key escrow techniques or outlawing cryptography, our Government may choose to take.

The technology shifts we are seeing here have interesting parallels to those in the field of radar. Since the beginning of World War II, radar has played an essential role in defending against attacks from the air. But recent technology shifts have produced stealth capabilities that for now, at least, effectively defeat radar. We will soon face an equivalent dilemma as stealth measures become widely available: how to prevent drug dealers, terrorists, and other adversaries from using them to enter our country undetected. We could require that all aircraft have some form of reflector that will guarantee that the Government can detect them whenever it has the need, but it is unlikely that those who wish to enter our airspace undetected will comply with such requirements.

We must recognize that those who wish to protect their communications from eavesdroppers will increasingly be able to do so. We must be careful not to continue to insist on misguided measures to try to retain decryption capability that will inevitably be eroded by technology, no matter how important we feel that capability may be.

The Congress Must Act Now!

The principal vehicle that the Government's law enforcement and national security interests have used to maintain the balance on their side of this dilemma over the years has been the imposition of strict export control measures on all cryptographic products leaving this country. In light of the ongoing and inevitable technological shift toward better protection mechanisms and increasing business communications needs, a review of this policy is urgently needed. Such a review must be conducted by someone willing to understand the needs of both sides of the issue. Based on our experiences to date, I am convinced that the U.S. Congress is the only organization with the authority and balanced perspective to tackle such a tough issue. I hope that these hearings will be the beginning of a true national debate of this most vital issue.

I would like to begin my testimony with a review of how these export controls came into place and why they made good sense in an earlier time but not necessarily now. I will then discuss the widespread and rapidly growing foreign availability of cryptographic products that is making this technological shift so hard for our intelligence capabilities. Following this, I will review the highly negative effect that U.S. export controls are having on U.S. industries and the average U.S. citizen.

WHY DO WE HAVE EXPORT CONTROLS ON CRYPTOGRAPHY?

The method that governments have used for most of this century to protect the privacy of their electronic communications and that has gradually become available to individuals throughout the world is called cryptography: the scrambling of data prior to transmission (encryption) and unscrambling upon receipt (decryption).

As governments came to rely upon cryptography to protect their vital communications, groups of highly skilled mathematicians were assembled by the same governments to attempt to break the encrypted communications of their adversaries.

In David Kahn's 1973 book, *The Codebreakers*, he states:

> Codebreaking is the most important form of secret intelligence in the world today. It produces much more and much more trustworthy information than spies, and this intelligence exerts great influence upon the policies of governments.

Few would argue that this statement remains just as true today as when it was written.

<u>Export Controls Were Essential Initially</u>

All modern governments face the difficult competing tasks of having good enough encryption capabilities to protect their own communications while trying to defeat the encryption capabilities of their adversaries. As encryption hardware devices became readily available, governments had to control where these devices went in order to limit the availability of good cryptography to hostile adversaries. Export control on encryption devices became an integral part of the Department of State munitions control process, where it remains today.

With the advent of computers, the ability to perform encryption functions using software programs rather than hardware made encryption more readily available and its export control more difficult. In the 1970s, efforts to improve the protection of domestic sensitive information led to publication of encryption algorithms such as the Federal Information Processing Standard (FIPS) Data Encryption Standard (DES) algorithm, which, while intended to be implemented only in hardware, quickly became available throughout the world in software.

Personal computers gave individual users direct access to the vast power of the computer and led to a revolution in how businesses operate. Now highly sensitive corporate plans and financial information flow freely over the phone lines among clusters of computers, and users are demanding improved security for their sensitive information from their software suppliers.

The natural result of this evolution is the need to include good quality encryption capabilities within modern software products for sale to multinational corporations worldwide. However, governments still want to control where encryption devices go in order to limit the availability of good quality encryption to hostile adversaries.

<u>But Times Have Changed</u>

So a problem that twenty years ago only affected governments and that led to the harsh export control restrictions presently in place on encryption now threatens the ability of U.S. citizens and businesses to protect their own sensitive information and the ability of the U.S. software industry to market the products that its multinational customers are demanding. This is truly a dilemma of national proportions that cannot be left solely in the hands of the national security interests to resolve.

Few would argue that the Government should not continue listening to the communications of its adversaries. But now that we have a worldwide economy with massive amounts of sensitive information flowing in all directions at all times, few are willing to give up the ability to provide reasonable protection to their own information in order to help the Government eavesdrop.

"Listening In" Will Keep Getting Harder

Even if we could forgo our personal and business privacy needs for the sake of the national security interests, the continuous evolution of technology has already made it harder to listen in to those who do not want to be heard than it was even a year ago. And that evolution will continue to make it even harder next year and in every year that follows.

The same technologies that have brought about the personal computer revolution are making good quality cryptography available worldwide, and those people, businesses, and governments that choose to protect their communications can now do so quite effectively and at reasonable cost. The task of listening in to others is becoming more and more difficult every day in spite of extensive export controls.

The widespread availability of encryption products worldwide will make it ever harder to decrypt the communications of adversaries who do not want to be heard, with or without excessive export control measures.

It is important to note that whether the U.S. Government drops export controls altogether on encryption products or attempts to impose absolute restrictions even on domestic use of encryption, the task of law enforcement and the national security community to listen in to our adversaries is going to get progressively harder day by day.

Now Export Controls Are Harmful to the Nation

Export controls served a useful purpose following World War II and up to the early 1980s. They protected the Government's interests and did not interfere with the interests of private citizens and commerce. Since cryptography has become an important tool for protecting the sensitive information of everyone, not just governments, and since the technology to implement good quality cryptography has now become readily available worldwide, export controls on good quality cryptography are no longer needed and are highly detrimental to the interests of the nation.

HOW WIDESPREAD IS CRYPTOGRAPHY WORLDWIDE?

Since the publication of the Data Encryption Standard as a U.S. Federal Information Processing Standard in 1977, cryptography has shifted from the exclusive domain of governments to that of individuals and businesses. DES in both hardware and software implementations is the de facto international standard against which all other algorithms are measured.

DES must be recertified as a FIPS every five years. In 1982, it was recertified without controversy. In 1987-1988, NSA recommended against recertification except for specialized use such as banking, but the recertification proceeded. This year the recertification is before the Secretary of Commerce awaiting approval. If approved, software implementations of DES will be allowed for the first time.

DES was adopted by the U.S. and international banking community shortly after its publication as a FIPS. The banking community fought for and obtained the right to export DES for financial uses, primarily integrity checks but also for banking confidentiality uses, and the right to generate their own keying material (the random numbers that initialize the encryption/decryption processes) without relying on any other Government agency.

In the mid 1980s, DES was proposed as an international standard by the International Standards Organization (ISO) as Data Encryption Algorithm-1 (DEA-1). Final approval was not made because of an appeal by the U.S. suggesting that the ISO should not approve any specific algorithms but leave that decision to individual nations.

The availability of DES and the controversy that arose as soon as it was published concerning whether it had weaknesses that NSA could exploit fostered the highly fruitful academic research into public key cryptography in the late 1970s. Public key algorithms have the major advantage that the sender does not need to have established a previous secret key with the recipient for communications to begin. Public key algorithms such as RSA have become as popular and widely used as DES throughout the world for integrity, confidentiality, and key management.

SPA Study of Availability of Cryptography

The Administration has asserted that export controls are not harming U.S. firms by causing them to lose market shares because there are no foreign products and programs available. Implementations of DES, RSA, and newer algorithms such as the International Data Encryption Algorithm (IDEA), an algorithm that has a key length more than twice that of DES, are available routinely on the Internet from sites all over the world. But according to the Administration, these do not count as commercial products.

In order to develop a definitive assessment of just how widespread cryptography is in the world, in May of this year, the SPA commissioned a study of products employing cryptography. There was a significant amount of knowledge about specific products here and there, but no one had ever tried to assemble a comprehensive database with, where possible, verification of product availability.

The SPA research team focused exclusively on products providing text, file, and data communications encryption capabilities and on programs and products using DES or its equivalent, i.e., the precise products subject to export restrictions. We did not include facsimile and voice encryption products. The team obtained information from product literature, reference guides, industry surveys, trade press and journal articles, and responses to requests for information from SPA members, cryptography experts, and information requests put on the Internet.

Whenever possible, the team followed up information with requests for product literature. This was carefully scanned by at least two independent project members, and the data was prepared for entry into the database. To the greatest extent possible, phone calls have been made to vendors to clarify ambiguous technical information.

Information on new products continues to flow in daily but as of October 12:

- We have identified 264 foreign hardware, software, and combination products for text, file, and data encryption from 21 foreign countries: Argentina (1), Australia (18), Belgium (8), Canada (16), Denmark (14), Finland (1), France (5), Germany (33), Hong Kong (1), India (1), Ireland (1), Israel (10), Japan (2), the Netherlands (15), New Zealand (1), Norway (1), Russia (8), South Africa (7), Sweden (17), Switzerland (18), and the United Kingdom (86).

- Of these 264 products, 123 employ DES.

- We have confirmed the availability of 58 foreign encryption software programs and kits that employ the DES algorithm. These are published by companies in Australia, Belgium, Canada, Denmark, Finland, Germany, Israel, the Netherlands, Russia, Sweden, Switzerland, and the United Kingdom. We know some have distributors in other foreign countries and in the United States; one, a UK company, has distributors in 13 countries (Bahrain, Denmark, France, Greece, Ireland, Italy, Malta, the Netherlands, Norway, Singapore, Spain, Sweden, and Yugoslavia). One in Germany has distributors in 14 countries (Australia, Austria, Belgium, Canada, France, Italy, the Netherlands, Norway, Spain, Sweden, Switzerland, Turkey, the UK, and the U.S.). The programs are installed by the user inserting a floppy diskette; the kits enable encryption capabilities to be easily programmed into a variety of applications.

A complete listing of all confirmed products in the database is identified in Attachment 1.

We have ordered and taken delivery on products containing DES from four countries: Denmark, Germany, Israel, and the United Kingdom.

Foreign customers increasingly recognize and are responding to the need to provide software-only encryption solutions. Although the foreign encryption market is still heavily weighted towards encryption hardware and hardware/software combinations, the market trend is towards software for reasons of cost, convenience, and space.

- On the domestic front, we have identified 288 products, of which 142 employ DES. Thus, at least, 142 products are unable to be exported, except in very limited circumstances, to compete with the many available foreign products.

- In total, we have identified to date 552 cryptographic products, developed or distributed by a total of 366 companies (211 foreign, 155 domestic) in at least 33 countries.

DES is also widely available on the Internet, and the recently popularized Pretty Good Privacy (PGP) encryption software program, which implements the IDEA, also is widely available throughout the world.

The ineffectiveness of export controls is also evident in their inability to stop the spread of technology through piracy. The software industry has a multibillion dollar worldwide problem with software piracy. Mass market software is easy to duplicate and easy to ship via modem, suitcase, laptop, etc. Accordingly, domestic software products with encryption are easily available for export--through illegal but pervasive software piracy--to anyone who desires them.

It cannot be any clearer: the existence of widespread and affordable cryptographic products overseas is an indisputable fact. Based on that fact, unilateral U.S. export controls keep U.S. firms from competing in the global marketplace.

Foreign customers who need data security now turn to foreign rather than U.S. sources to secure that need. As a result, the U.S. Government is succeeding only in crippling a vital American industry's exporting ability.

Following the first publication of the cryptographic database at the Advisory Board meeting on June 2, the Administration requested a meeting with the SPA research team to review their approach and findings. This meeting was held on July 1, 1993, at the Department of Commerce and involved Government representatives from the Department of Commerce and NSA. The team described both their technique for gathering and cataloging the information and the latest results. At the conclusion of the meeting, it appeared that the Administration representatives were satisfied that a valid survey process was being carried out.

At the second meeting of the Advisory Board on July 29, a Government representative of the Administration indicated that the mere availability of products overseas was not sufficient, that what was needed was an assessment of the market impact of those products. It is important to note to the contrary, though, that the Department of Commerce, in similar deliberations, requires only the demonstrated existence of foreign products, not an assessment of their market share. It would seem that no matter how much information is acquired at what level of detail, the Administration will request more to delay further action.

Nevertheless, the study begun in May by the SPA will continue to collect additional information on cryptographic product availability and to periodically publish its results to help focus attention on this important and often ignored situation. We would welcome Government participation in this ongoing effort to ensure the maximum coverage of available products and maximum utility to the Government.

Frequently Heard Arguments

One argument that is frequently heard to justify continued export controls is that cryptographic products are not available outside the U.S. so U.S. software and hardware developers are not hurt by export controls. The statistics from the SPA survey (264 foreign products, 123 using DES) prove that this argument is patently false!

A second argument is that even if products are available, they cannot be purchased worldwide. This is also patently false!

We have found 366 companies in 32 foreign countries and the U.S. that are manufacturing, marketing, and/or distributing cryptographic products, most on a worldwide basis. The names of these companies are listed in Attachment 2.

A third argument frequently heard is that the products sold in other parts of the world are inferior to those available in the U.S. Again, the results of our survey show this to be patently false!

We purchased products from several sources throughout the world. We ordered DES-based PC file encryption programs for shipment using routine channels from:

- Algorithmic Research Limited (ARL), Israel
- Sophos Ltd., UK
- Cryptomathic A/S, Denmark
- CEInfosys GmbH, Germany
- uti-maco, Germany
- Elias Ltd., Russia (distributed through EngRus Software International, UK)

All the products we ordered were shipped to us in the U.S. within a few days. The German products were sent to us directly from their U.S. distributors in Virginia and Connecticut, respectively. Our experience has been that if there is paperwork required by the governments in which these companies operate to approve cryptographic exports, it is minimal and results in essentially immediate approval for shipping to friendly countries.

The products we obtained from these manufacturers and distributors were in every case first rate implementations of DES. To better understand if foreign products are somehow inferior, we tried to order the same Sophos product from their Bahrain distributor. We were informed by the distributor that since we were outside his area, he could not sell directly to us. He then told us that everything he sells is shipped directly from the manufacturer in England.

The uti-maco U.S. distributor in Connecticut indicated that he could ship us his German made product immediately (we received it the next day), without needing any further approval from the German parent company or the German government. Apparently, the Germans have a form of blanket approval for sale to anyone in the U.S. I asked if that was true elsewhere in the world and the representative told me that while he dealt only in the U.S., he believed that this was true.

We have no indication that products being shipped to the U.S. or the rest of the world from foreign manufacturers or distributors are in any way inferior to products available in the U.S.

Others Use Different Rules

But our survey results also point to a much more ominous finding! Apparently the controls imposed by the U.S. Government on export of cryptographic products from the U.S. are far more restrictive than those imposed by most other countries including our major allies. The effect of this most unfortunate situation is to cripple U.S. industry while our friends overseas are essentially free to export as they wish.

The U.S. imposes very strict rules on the export of cryptographic products. In general, applications for the export of products that use DES will be denied even to friendly countries unless they are for financial uses or for U.S. subsidiaries. We have been told repeatedly by the U.S. Government that other countries such as the United Kingdom and Germany have the same export restrictions that the U.S. does.

But our experiences with these purchases of cryptographic products show a very different picture.

Companies in the UK, Germany, Denmark, and Israel can freely ship DES products to the U.S. and presumably elsewhere in the world with no more then a few days of government export control delay, if any. The claim is they have to "fill out some papers," but it's no big problem.

Based on our experiences to date, I conjecture that these countries are using CoCom (the Coordinating Committee of western nations and Japan) rules for determining where to allow exports. If this conjecture is true, most countries in the free world can readily receive exports from these countries. I speculate that companies in these countries are required to fill out export forms but if they can show that the destination country is not proscribed by CoCom or their local equivalent, they can ship without waiting for further government approval. Every experience we have had supports this supposition.

Whether my theory is correct or not, our experience with these purchases has demonstrated conclusively that U.S. business is at a severe disadvantage in attempting to sell products to the world market. If our competitors overseas can routinely ship to most places in the world within days and we must go though time consuming and onerous procedures with the most likely outcome being denial of the export request, we might as well not even try. And that is exactly what many U.S. companies have decided.

And please be certain to understand that we are not talking about a few isolated products involving encryption. More and more we are talking about major information processing applications like databases, electronic mail packages, and integrated software systems that must use cryptography to provide even the most basic level of security being demanded by multinational companies.

Demonstrations of Available Cryptographic Products

We have before us today several examples of cryptographic products that were lawfully obtained in the United States from foreign vendors:

- AR DISKrete: produced by Algorithmic Research Limited (ARL), Israel.
  Uses DES disk/file encryption to provide PC security and access control.

- EDS: produced by Sophos Ltd., UK.
  DES-based PC file encryption package.

- F2F (File-to-File): produced by Cryptomathic A/S, Denmark.
  DES-based PC file encryption utility.

- Softcrypt: produced by CEInfosys GmbH, Germany.
  DES-based PC file encryption utility.

- SAFE-GUARD Easy: produced by uti-maco, Germany.
  DES-based PC file encryption utility.

- EXCELLENCE for DOS: produced by Elias Ltd., Russia distributed through EngRus Software International, UK.
  GOST-based (Russian DES equivalent) PC file encryption utility.

We also have a demonstration of the power of the digital revolution and the impact it will have on all our communications in the future. Traditionally, when we think of voice communications, we think of the telephone in its many forms (desk, cordless, cellular, car). However, many modern computer workstations now have the ability to carry voice as well as other multimedia communications. Routinely today on the Internet, voice conferences are held over packet switched communications networks.

Today we have a demonstration using two workstations that come with software to digitize voice communications, packetize it for transmission over a network, and resynthesize it into perfectly good (sometimes better than phone quality) voice. Systems like these are being used daily for voice conferencing over networks around the world.

With this capability, it is straightforward to protect phone conversations from eavesdroppers. Since all the capabilities are performed in software, it is trivial to add an encryption algorithm, such as the Data Encryption Standard, to the software and provide good quality encryption to the digitized, packetized speech. Today we have DES versions from Finland, Sweden, Australia, and the U.S.

HOW IS U.S. INDUSTRY BEING AFFECTED BY EXPORT CONTROLS?

TIS Experiences

To begin this section, I would like to give several examples of experiences that my company has had recently in dealing with the export control process.

Trusted Information Systems is a member of the Internet community and has implemented a version of the Internet Privacy Enhanced Mail (PEM) system, which it is offering free to users on the Internet and for sale to commercial users under the name Trusted Mail™. Several hundred Internet users have retrieved the PEM source code, and many of them are using it on a daily basis. Our experiences with PEM illustrate the variety of frustrations, confusion, and lost opportunities that confront U.S. businesses in the area of international cryptographic products.

PEM is based on international Internet specifications developed over the past five years by a team of researchers from throughout the world. In its present version, PEM uses DES for confidentiality and RSA for signature and key management. As such, it does not meet the U.S. Department of State requirements for export outside the U.S. or Canada.

In order to establish a distribution system for PEM similar to that of other software products on the Internet, TIS reviewed various techniques that universities and other companies have used. The "anonymous FTP" approach, in which a user who does not have an account is allowed to log on to the computer containing the information and perform a file transfer of the specific program files, was considered the best choice. Such techniques are routinely used throughout the Internet, but in the case of software that is subject to export controls, one must be concerned that individuals outside the U.S. and Canada may attempt to retrieve the programs. The problem is how to identify whether someone who is anonymous is approved to retrieve the software or not.

As had been done earlier by others, we have created a "READ ME" file that the person seeking the software must read before retrieving the PEM program. The reader is cautioned that if he or she is not from the U.S. or Canada, it is against U.S. export law to proceed. The file name of the PEM programs contained in the "READ ME" file is changed frequently to force the anonymous user to read the export control caution. We also installed filters that automatically refuse requests that are clearly coming from outside the U.S. or Canada. But we know that those filters cannot stop inquiries from foreign sources that have accounts in the U.S. To the best of our knowledge, our approach is as sound as many that others are using and better than most.

Before we put the system on line, though, we sought the approval of the Department of State and the National Security Agency. Initially we got acknowledgements to our phone calls describing our problem and proposed solution. We were told orally at one time that because the PEM software was "free," it was permissible to proceed this way, implying that if we charged for it, somehow this process would not be approved. But as we began to seek official approval for this process, we received fewer and fewer responses. Our inquiries finally took the form of: "Unless you tell us not to do this, this is how we intend to proceed." On June 1, 1993, we put the anonymous FTP process on line, and our system has responded to hundreds of requests. We have never received acknowledgement that the process is either acceptable or unacceptable to the Government despite being told on several occasions that we would receive such acknowledgement.

The above described process is patterned after a similar process that takes place now in software retail stores. Programs for sale over the counter containing DES or similar export controlled software are supposed to be marked with explicit and obvious labels telling the buyer that these products cannot be taken from the U.S. or Canada. The burden of complying with the export laws rests entirely with the buyer since the seller has no responsibility to ascertain whether the buyer is a U.S. or Canadian citizen. One has to wonder if these prominent notices, rather than advising buyers to beware, do not guide the foreign buyer, who is not concerned with violating U.S. export laws, directly to the product he or she wishes to buy.

A second situation of interest involves a potential major customer of PEM, the British Ministry of Defence (MoD). For several years, TIS has been discussing PEM with officials in the MoD for use with unclassified information among MoD users and their industrial suppliers. TIS has a perfectly good solution to MoD's problems and could have had it running there years ago. Unfortunately, we cannot export PEM even to the British MoD because PEM uses the DES and RSA encryption algorithms.

Last year, the SPA succeeded in obtaining expedited export approval for software products that use cryptography so long as the key length is 40 bits or less. While this was a significant accomplishment, since it was the first time that any cryptography for confidentiality was given general export approval, the victory was short lived. Forty-bit key algorithms can be exhaustively searched in very short times. If a device could be built to exhaustively search a 56-bit key space (DES) in 176 years, it would take less than 1 day to search a 40-bit key space. Foreign customers for U.S. products who already have DES readily available laughed at the 40-bit U.S. restriction. TIS produced a 40-bit version of Trusted Mail and obtained the expedited Department of State export approval but to date has been unable to find a foreign (or domestic) customer willing to accept the weak 40-bit key length.

After spending much energy searching for plausible solutions to this problem, our newly formed Trusted Information Systems (UK) Limited office has contracted with British scientists to implement a new UK version of PEM based on the same international specifications and using DES and RSA algorithms that are already available in the UK. In a very real sense, this situation demonstrates that the only accomplishment of U.S. export control restrictions is the export of U.S. jobs.

To make matters even worse (in the job export sense, at least), because of provisions in the UK export laws, it appears that we can *import* the UK product for sale in the U.S., something we would never be able to do in reverse.

These examples of problems with the export control process or its consequences are typical of the situations many U.S. companies find as they attempt to enter the world of software cryptography.

<u>Industrywide Experiences</u>

Some companies do try to compete and offer excellent DES-based products in the U.S. But because of the export restrictions, they must develop weaker versions for export if they wish to pursue foreign markets. Many companies forgo the business rather than spend extra money to develop another inferior product that cannot compete with products widely available in the market.

The Government already has a measure of lost sales and dissatisfied customers in the number of State Department/NSA export license applications denied, modified, or withdrawn. However, it is impossible to estimate accurately the full extent of lost sales. Many potential customers know that U.S. companies cannot meet their demand and thus no longer inquire. Conversely, some companies have given up even trying to get export approvals for DES to meet customer demand.

Gauging the extent of economic harm to companies is an inherently difficult task because most companies do not want to reveal that sort of information. Consequently, there exists only anecdotal information. But the accumulation of anecdotal information collected by the SPA paints a picture of three ways in which the export controls on cryptographic products are hurting American high-tech industry.

(1) First, for many data security companies, every sale is vital, and the loss of contracts smaller than $1 million can often mean the difference between life and death for these companies. The confusion and uncertainty associated with export controls on encryption generate severe problems for small firms, but not as severe as the loss of business they suffer from anti-competitive export controls. Examples abound:

- One U.S. company reported loss of revenues equal to a third of its current total revenues because export controls on DES-based encryption closed off a market when its customer, a foreign government, privatized the function for which the encryption was used, and the U.S. company was not permitted to sell to the private foreign firm. The company estimates it loses millions of dollars a year because it receives substantial orders every month from various European customers but cannot fill them because of export controls.

- One small firm could not sell to a European company because that company sold to clients other than financial institutions (for which export controls grant an exception). Later, the software firm received reports of sales of pirated copies of its software. This constituted a loss of a $400,000 contract for the small U.S. software firm.

- Because of existing export restrictions, an American company recently found itself unable to export a mass market software program that provided encryption using Canadian technology based on a Japanese algorithm. Yet other European and Japanese companies are selling competing products worldwide using the same Canadian technology.

- An SPA member's product manager in Europe reported the likely loss of at least 50% of its business among European financial institutions, defense industries, telecommunications companies, and government agencies if present restrictions on key size are not lifted.

- Yet another SPA member company reported the potential loss of a substantial portion of its international business if it cannot commit to provide DES in its programs.

- A German firm that opened a subsidiary in the U.S. sought a single source encryption software product for both its German and U.S. sites. A U.S. data security firm that bid for the contract lost the business because U.S. export controls required that the German firm would have to wait approximately six months while a license was processed to sell them software with encryption for foreign application. The license could only be for one to three years, the three year license being more expensive. Consequently, the German firm ended up purchasing a DES-based system from another German company, and the U.S. firm lost the business.

- A foreign government selected one software company's data security product as that government's security standard. The company's application to export the DES version was denied, and as a consequence the order was lost. This cost the company a $400,000 order and untold millions in future business.

(2) Second, multinational corporations (MNCs) are a prime source of business in the expanding international market for encryption products. Many U.S.-based firms have foreign subsidiaries

or operations that do not meet export requirements. While U.S. products may be competitive in the U.S., many MNCs obtain from foreign sources encryption systems that will be compatible with the company's worldwide operations. Moreover, foreign MNCs cannot rely on the availability of U.S. products and have been known to import foreign cryptography for use in their U.S. operations.

- One U.S. firm reports the loss of business from foreign MNCs that will not integrate the company's products into their U.S. operations because of the export restrictions that would prevent them from being compatible with their domestic operations.

- The Computer Business Equipment Manufacturers Association reports that one of its members was denied an export license and lost a $60 million sale of network controllers and software for encryption of financial transactions when the Western European customer could not ensure that encryption would be limited to financial transactions.

(3) Third, encryption systems are frequently sold as a component of a larger system. These "leveraged" sales offer encryption as a vital component of a broad system. Yet the encryption feature is the primary feature for determining exportability. Because of the export restrictions, U.S. firms are losing the business not just for the encryption product but for the entire system because of the restrictions on one component of it.

- One data security firm has estimated that export restrictions constrain its market opportunities by two-thirds. Despite its superior system, it has been unable to respond to requests from NATO, the Swedish PTT, and British telecommunications companies because it cannot export the encryption they demand. This has cost the company millions in foregone business.

- One major computer company lost two sales in Western Europe within the last 12 months totaling approximately $80 million because the file and data encryption in the integrated system was not exportable.

One possible solution to the problem of export controls may be for U.S. companies to relocate overseas. Some U.S. firms have considered moving their operations overseas and developing their technology there to avoid U.S. export restrictions. Thus, when a U.S. company with technology that is clearly in demand is kept from exporting that technology, it may be forced to export jobs instead.

HOW ARE U.S. CITIZENS AND BUSINESSES BEING AFFECTED BY ALL THIS?

The answer to this question is painfully simple. When U.S. industry forgoes the opportunity to produce products that integrate good security practices, such as cryptography, into their products because they cannot export those products to their overseas markets, U.S. users (individuals, companies, and Government agencies) are denied access to the basic tools they need to protect their own sensitive information. This is where the greatest frustration sets in.

The U.S. Government established export controls in order to keep good quality cryptography from proliferating outside the U.S. The result has been exactly the opposite effect. Good quality cryptography is now available everywhere in the world including the U.S. But U.S. customers cannot buy it integrated into the information system products they normally use because U.S. export laws discourage U.S. suppliers from developing such products.

We seem caught in a vicious circle that appears to make sense only to those who do not want to see good quality cryptography used anywhere.

WHAT EFFECT WILL CLIPPER HAVE?

In the midst of all of this, on April 16, 1993, the President announced the Clipper initiative to ensure the public's right to privacy while allowing law enforcement to conduct lawful wiretaps.

The principal concern of many with Clipper is the potential it has for violating the privacy of citizens. In his April 16 announcement, the President stated that "The Administration is committed to policies that protect all Americans' right to privacy while also protecting them from those who break the law." It would appear that the only way both aspects of this policy can be carried out is if the individual's right to privacy is superseded by the Government's right to listen in whenever the Government chooses. Many people fear that this isn't much of a right to privacy.

There are many other concerns that have been expressed about the Administration's Clipper Initiative and the negative aspects of key escrow. But with respect to the issue of export restrictions on software products, Clipper represents primarily a distraction only serving to cloud the issues. Unless Clipper is made mandatory, its requirement to use hardware and its key escrow provisions will cause it to have little impact on the software market. No one will willingly give up the convenience of integrated software encryption for an expensive hardware box that will let the Government listen in.

The international aspects of Clipper are not at all thought out. Even if Clipper were exportable, the fact that the U.S. Government will hold the keys and not share them with other governments ensures that this will be no more successful overseas than the 40-bit key length "solution."

Clipper is a major diversion that does not solve any of the problems discussed above.

WHAT CAN BE DONE?

Many Calls for Action

Many people have been clamoring about the need to relax export controls on encryption for years. The National Research Council has recently issued four reports expressing serious concern in this area (Attachment 3).

The computer industry has been complaining ever more loudly for ten years.

The Congressionally chartered Computer System Security and Privacy Advisory Board has called for a national review of these issues involving Government (civilian, law enforcement, and national security interests) and industry (users and vendors). The Advisory Board passed resolutions on the need for a national review and expressing serious concerns about the Clipper Initiative (Attachment 4).

The Administration has formed an Interagency Review at the request of the President to look at all aspects of the cryptography issue including export control. This review is the highest level investigation of this problem to date. Its report is due out any time, within days or weeks. Unfortunately, the review is being conducted from behind closed doors with the only public input coming through the auspices of the Advisory Board and such industry groups as the Digital Privacy and Security Working Group.

Since the Interagency review began with the Clipper announcement and is being conducted by Government officials who are heavily committed to Clipper, it is unlikely that its results will assist business by easing the software cryptography export control constraints.

President Clinton, in commenting on the North American Free Trade Agreement, was quoted by the *Washington Post*, September 16, 1993, as saying:

> I'm telling you folks, we cannot repeal the force that is driving the world economy together. We can run away from it and get beat by it, or we can embrace it, do what we have to do and win with it.

If only those who control cryptographic exports understood this.

On September 30, the President announced a significant relaxation of the export control rules for high performance computer technology. It would be good if some of that change could affect the cryptography export area, but the present export position is so well entrenched, it is unlikely there will be much change from the Executive Branch.

The Congress Must Act Now!

The only hope for a recognition of the counterproductive nature of this situation is in the Congress. No other organization has the breadth of constituencies to allow an honest look at all the concerns and the authority to come to a definitive resolution on the issue.

We need to recognize that the U.S. public has a right to a reasonable level of protection for its sensitive information. Enabling that right through allowing the export of good quality cryptography such as DES will not harm the intelligence gathering capabilities of this country any more than the worldwide proliferation of cryptography already has.

I strongly encourage this Subcommittee to press as vigorously as possible for legislation that will allow the export of good quality cryptography so that our industry will implement it and our citizens can use it!