NOTE: CHARTS 1 THROUGH 4 ARE NOT INCLUDED IN THIS DOCUMENT

ORAL 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 are having on one of the few industries where the U.S. remains dominant worldwide, the information system software industry.

My name is Steve Walker. I am the founder and President of Trusted Information Systems (TIS), Inc., a ten year old small business with offices around the U.S. and in England, specializing in research, product development, and consulting in information 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 with the Department of Defense, at the National Security Agency, the Defense Advanced Research Projects Agency, and the Office of the Secretary of Defense. My last job with the Government was as Director of Information Systems for the Assistant Secretary of Defense for Communications, Command, Control, and Intelligence (C3I).

I have been a member of the Computer System Security and Privacy Advisory Board (CSSPAB), chartered by the Computer Security Act of 1987, throughout its many deliberations on cryptography.

My written testimony describes the national dilemma between, on the one hand, the interests of law enforcement and national security to limit the availability of good quality cryptography so they can continue to listen in to our adversaries and, on the other hand, the rapidly growing interests worldwide of individuals and businesses to protect their sensitive information.

The tension between these forces has been building for years and is reaching crisis stage. But the arguments on both sides have been mostly gloomy predictions of disaster: from the Government if we were to open up exports of cryptography, and from industry if we don't.

I am very pleased today to be able present some concrete evidence that may begin to move this debate from a war of words to the careful analysis of factual information that is so badly needed.

SPA Survey of Available Cryptography

In May 1993, the SPA chartered a survey of the worldwide availability of good quality cryptography. The findings to date indicate that cryptography is available now to essentially anyone who wants it.

[PUT UP CHART 1 # SUMMARY]

Within just five months of part-time effort by a few dedicated people, we have confirmed product literature and in a few cases actual software for 200 foreign products, 123 using the Data Encryption Standard algorithm, the official U.S. and defacto worldwide encryption standard. We have leads that we are confirming on another 64 foreign products, giving a total of 264 products developed and available outside the U.S.

We have found manufacturers of cryptographic products in 21 foreign countries and distributors of cryptographic products in 33 countries throughout the world.

[PUT UP DISTRIBUTORS MAP, EASEL 2]

Most of the major countries of the western world are represented here.

In the course of the survey, we have also confirmed the availability of 241 cryptographic products in the U.S., 142 using DES, and we are attempting to confirm 47 others. Worldwide, we have identified 552 products overall. The names and countries of origin of these products are listed in Attachment 1 of my testimony.

We are continuing to find more products, manufacturers, and distributors on a daily basis. We believe we have just scratched the surface.

We have assembled a set of notebooks that contain the product descriptions of all confirmed products in our database. We also have some of the sources of the information we have used to find these products. In addition, we have several of the products that we have purchased to confirm that good quality cryptography is indeed available worldwide.

Frequently Heard Arguments

There are a series of arguments that are frequently heard from those who wish to justify continued export controls.

The first one is, "Cryptographic products are not available outside the U.S. so U.S. software and hardware developers are not hurt by export controls." We believe our survey results have already proven that statement to be patently false!

A second argument is, "Even if cryptographic products are available, they cannot be purchased worldwide." Our survey results show that 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 of my testimony.

A third argument frequently heard is, "Even if the products are available and can be purchased easily, those sold in other parts of the world are somehow inferior to the products available in the U.S." To the contrary, the results of our survey show that foreign products are just as good and in many cases better than many U.S. products.

We purchased products from several sources throughout the world. We ordered DES-based PC file encryption programs for shipment to the U.S. from:

- Algorithmic Research Limited, of Israel
- Sophos, Ltd, of the United Kingdom

- Cryptomathic A/S, of Denmark
- CE Infosys Gmbh, of Germany
- uti-maco, of Germany

We also obtained a similar product from:

- Elias Ltd., of Moscow, Russia (distributed through EngRus Software International, UK. This product uses GOST, the Russian equivalent of DES.)

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 export approval paperwork required by the governments of these companies, 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 good products were being shipped to the U.S. and inferior products being sold overseas, we ordered the same Sophos product that we already had from their Bahrain distributor. We were told by the distributor that everything he sells is shipped directly from the manufacturer in England.

The uti-maco U.S. distributor in Connecticut shipped us his German made product within a day and without needing any further approval from the German parent company or the German government. Apparently, they have some form of blanket approval for sale to anyone here. I asked if that was true elsewhere in the world and the representative told me, while he dealt only in the U.S., he believed that this was the case.

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.

In many cases the products have proven to be of superior quality, easily comparable with U.S. products.

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.

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. [COCOM MAP, EASEL 3]

[PUT UP COCOM MAP NOW]

This chart illustrates in red the CoCom proscribed countries plus a set of terrorist countries. All of the countries in Green are apparently available for export with minimal restrictions.

If this conjecture is true, it explains why these countries can readily ship to most countries in the free world. I speculate that companies in these countries may be 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 with the survey supports this supposition. If only this were true in the U.S.!

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.

AT&T Products

We also have a collection of products manufactured by or for AT&T for sale in the U.S. and in some cases overseas. These include telephone security devices, facsimile security devices, and data communications devices. Some of these devices are intended to be made with the Administration's Clipper Chip whenever it becomes available, but all of them are available NOW with either DES or proprietary encryption algorithms. Some of these devices are manufactured in Switzerland. They can be imported into the U.S. for sale, but they cannot be exported elsewhere. Indeed, if they break they cannot be returned to the manufacturer for repair.

Demo

We now have a brief demonstration of just how available cryptography is and how easily it can be applied to protect sensitive information anywhere in the world.

We have here two commercially available computer workstations running commercially available software and connected by a conventional network (or dialup line). They are communicating audio information (in this case from a tape recorder) much as is done daily by voice conferences on the Internet. The delay you hear is being emphasized for purposes of the demonstration. Everything being shown here is commercially available today throughout the world.

[ADD FIRST CRYPTO TO BOTH SYSTEMS]

We can now add a software version of DES from Australia to both the sender and receiver stations to add good quality encryption to the communications.

[PUT INCORRECT KEY IN RECEIVING WORKSTATION]

Now if Dave wanted to keep Pete from listening in to his music, he could change the key used for the encryption and demonstrate what an interceptor might hear.

Next we reset the key so we can communicate again.

[USE SECOND DES VERSION ON BOTH WORKSTATIONS]

Now we can demonstrate this using a Swedish DES implementation. There is no difference in the result.

There is no rocket science involved here. Anyone with an elementary knowledge of modern computer workstations can do what we have done. All of the software is available essentially anywhere in the world. We must not kid ourselves about this being difficult or unavailable!

PEM Experiences

My written testimony lists many of the experiences of U.S. companies that the SPA has collected. I would like to discuss briefly my company's experiences with one of our products, Privacy Enhanced Mail. PEM is a software product that works with electronic mail systems to add encryption services for secrecy and authentication. PEM is capable of using a wide variety of encryption algorithms but in its Internet version uses DES and therefore cannot be exported except to Canada.

We have been discussing PEM with the British government for several years. We have a product that could have already been in wide use there, satisfying their unclassified electronic mail protection needs, except that we cannot export it to them. When the SPA successfully negotiated an agreement with NSA last year allowing the export of encryption products with short key lengths (40 bits or less), we approached the British with an exportable version of PEM. Since DES (with its 56-bit key length, 65,000 times stronger than our 40-bit exportable version) is already widely available in the UK, the British politely informed us that they did not want to consider such a weak product.

To attempt to satisfy our British customers, we have recently hired British scientists to implement an independent version of PEM using the published international specifications and UK versions of DES. The impact on TIS involves the cost of reimplementing something we already have, plus the loss to the U.S. of sales of approx 10,000 systems, roughly $2.5 million over several years. This represents a revenue impact to my company of between 15 and 25% of our total revenue in any given year.

But the ironic part of this is that because of the apparent differences between the UK export laws and those imposed by the U.S., we may be able to import the UK PEM implementation for sale in the U.S. and thus eliminate the need for our U.S. PEM operation all together.

Unfortunately, these experiences are not unique to my company. Similar and all too often worse stories abound throughout the U.S.

Why?

And why is all this happening? U.S. law enforcement and national security interests are trying to retain the ability to intercept the communications of our adversaries in the face of accelerating technology shifts that will make it ever easier for those who wish to protect their communications to do so.

I do not wish to deny the Government the right, indeed the responsibility, to try as hard as they can to maintain that ability. But we must recognize the total magnitude of this problem. We must find a way to balance the costs to the citizens of the United States of losing its vital industrial secrets to foreign espionage and its dominant position in the information processing industry to foreign competition versus the inevitable reduction of our interception capabilities, when foreign availability of cryptography is already so great.

Calls for Action

The National Research Council has warned of this problem in four recent reports (see Attachment 3 of my testimony). The Computer System Security and Privacy Advisory Board has called for a national review of this dilemma for nearly two years (see Attachment 4 of my Testimony). The President said, on September 16, that "...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."

On September 30, the President announced a dramatic relaxation of the export controls on all types of high performance computer products. Is it not time to look at the exports of cryptographic products, too? If we don't, the National Information Infrastructure will very likely get its security protection from foreign sources.

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 urge this Subcommittee to press vigorously for legislation to allow the export of good quality cryptography so that our computer industry will build it into their products and our citizens can use it to protect their vital sensitive information.