S. HRG. 106-892

S. 798, THE PROMOTE RELIABLE ON-LINE TRANSACTIONS TO ENCOURAGE COMMERCE AND TRADE (PROTECT) ACT OF 1999

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED SIXTH CONGRESS

FIRST SESSION

JUNE 10, 1999

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PRINTING OFFICE

69–984 FDP WASHINGTON : 2002

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED SIXTH CONGRESS

FIRST SESSION

JOHN MCCAIN, Arizona, *Chairman*

TED STEVENS, Alaska
CONRAD BURNS, Montana
SLADE GORTON, Washington
TRENT LOTT, Mississippi
KAY BAILEY HUTCHISON, Texas
OLYMPIA J. SNOWE, Maine
JOHN ASHCROFT, Missouri
BILL FRIST, Tennessee
SPENCER ABRAHAM, Michigan
SAM BROWNBACK, Kansas

ERNEST F. HOLLINGS, South Carolina
DANIEL K. INOUYE, Hawaii
JOHN D. ROCKEFELLER IV, West Virginia
JOHN F. KERRY, Massachusetts
JOHN B. BREAUX, Louisiana
RICHARD H. BRYAN, Nevada
BYRON L. DORGAN, North Dakota
RON WYDEN, Oregon
MAX CLELAND, Georgia

MARK BUSE, *Staff Director*
MARTHA P. ALLBRIGHT, *General Counsel*
IVAN A. SCHLAGER, *Democratic Chief Counsel and Staff Director*
KEVIN D. KAYES, *Democratic General Counsel*

C O N T E N T S

WITNESSES

S. 798, THE PROMOTE RELIABLE ON-LINE TRANSACTIONS TO ENCOURAGE COMMERCE AND TRADE (PROTECT) ACT OF 1999

THURSDAY, JUNE 10, 1999

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The committee met, pursuant to notice, at 9:32 a.m. in room SR–253, Russell Senate Office Building, Hon. Conrad Burns presiding.

Staff members assigned to this hearing: David Crane, Republican professional staff; and Gregg Elias, Democratic senior counsel.

OPENING STATEMENT OF HON. CONRAD BURNS, U.S. SENATOR FROM MONTANA

Senator BURNS. We will call the committee to order this morning, and thank you for coming. We will try to get started on time here.

Let me apologize for the chairman of the full committee, John McCain. He has a bill on the floor, the Y2K bill. I told him that he probably put the fox in charge of the henhouse here when he lets me chair this hearing, but it is something that I have been very much interested in for a long time.

Today's hearing will focus specifically on the "PROTECT Act of 1999." This bill reflects a number of discussions the full Committee chairman and I have had about the importance of encryption in the digital age. I would also like to thank Senator Wyden and Senator Abraham for their instrumental role in the creation of this pro-encryption legislation that I am confident will be supported by the large majority of this committee.

Along with several other members of this committee, I have long advocated the enactment of legislation that would facilitate the use of strong encryption. Strong encryption is necessary if we are to promote electronic commerce, secure our confidential business and our sensitive personal information, to prevent crime and to protect our national security by protecting our commercial information systems.

Beginning in the 104th Congress, I introduced legislation that would ensure the private sector continues to take the lead in developing innovative products to protect the security and confidentiality of electronic information, including the ability to export such American products, and I believe PROTECT accomplishes these important objectives. Specifically, the bill does the following:

It permits the immediate exportability of strong encryption products whenever foreign products contain the same strength of

encryption are generally available. It prohibits domestic controls on the use of products using strong encryption. It also guarantees that American industry will continue to be able to come up with new and innovative products.

It immediately decontrols encryption products using key lengths of 64 bits or less. It permits the immediate exportability of 128-bit encryption in all encryption products to a broad group of users.

Today we are in a world that nearly everyone has a computer and those computers are for the most part connected to one another. In light of that fact, it is becoming more and more important to ensure that our communications over these computer networks are conducted in a secure way.

It is no longer possible to say that when we move into the information age we will secure these networks, because we are already there. We use computers in our homes and our businesses in ways that we could not imagine only 10 years ago. These computers are connected through networks, making it easier to communicate than ever before.

This phenomenon holds promise for transforming life in a bunch of areas in our country and especially in Montana, where health care and state-of-the-art education can be delivered over networks to people located in remote population centers. These new technologies can improve the lives of real people, but only if the security of information that moves over these networks is safe and reliable.

The problem today is that our computer networks are not as secure as they could be. It is fairly easy for amateur hackers to break into our networks. The newspaper has been full of those kind of activities for the last year. They can intercept information, steal trade secrets and intellectual property, or even alter medical records.

The solution to this problem is to let individuals and businesses alike take steps to secure that information. Encryption is a vital tool which helps to protect the integrity of these electronic networks which have made so many modern wonders available in this age.

I look forward to the testimony of our witnesses today because this is a critical issue.

Now I would like to recognize the Senator from Massachusetts, Senator Kerry, and thank you for coming this morning.

[The prepared statement of Senator Burns follows:]

PREPARED STATEMENT OF HON. CONRAD BURNS, U.S. SENATOR FROM MONTANA

I am pleased to chair today's hearing in the Full Committee, which is on a topic critical to the future of this country—reforming our country's severely outdated encryption policy. Today's hearing will focus specifically on the "PROTECT Act of 1999." This bill reflects a number of discussions the Full Committee Chairman and I have had about the importance of encryption in the digital age. I would also like to thank Sen. Wyden and Sen. Abraham for their instrumental role in the creation of this pro-encryption legislation that I am confident will be supported by a large majority of this Committee.

Along with several other members of this Committee, I have long advocated the enactment of legislation that would facilitate the use of strong encryption. Strong encryption is necessary to promote electronic commerce, secure our confidential business and sensitive personal information, prevent crime and protect our national security by protecting our commercial information systems. Beginning in the 104th Congress, I introduced legislation that would ensure that the private sector con-

tinues to take the lead in developing innovative products to protect the security and confidentiality of our electronic information including the ability to export such American products. I believe PROTECT accomplishes these important objectives.

Specifically, the bill does the following:

• Permits the immediate exportability of strong encryption products whenever foreign products containing the same strength of encryption are generally available;

• Prohibits domestic controls on the use of products using strong encryption;

• Guarantees that American industry will continue to be able to come up with innovative products;

• Immediately decontrols encryption products using key lengths of 64 bits or less; and

• Permits the immediate exportability of 128 bit encryption in all encryption products to a broad group of users.

Today, we are in a world where nearly everyone has a computer and that those computers are, for the most part, connected to one another. In light of that fact, it is becoming more and more important to ensure that our communications over these computer networks are conducted in a secure way. It is no longer possible to say that when we move into the information age, we'll secure these networks, because we are already there. We use computers in our homes and businesses in a way that couldn't have been imagined 10 years ago, and these computers are connected through networks, making it easier to communicate than ever before. This phenomenon holds the promise of transforming life in states like Montana, where health care and state-of-the-art education can be delivered over networks to people located far away from population centers. These new technologies can improve the lives of real people, but only if the security of information that moves over these networks is safe and reliable.

The problem today is that our computer networks are not as secure as they could be. It is fairly easy for amateur hackers to break into our networks. Hackers can intercept information, steal trade secrets and intellectual property or even alter medical records. The solution to this problem is to let individuals and businesses alike to take steps to secure that information. Encryption is a vital tool which helps to protect the integrity of these electronic networks which have made so many wonders of the modern age possible.

I look forward to the testimony of the witnesses on this critical issue.

Thank you.

STATEMENT OF HON. JOHN F. KERRY, U.S. SENATOR FROM MASSACHUSETTS

Senator KERRY. Mr. Chairman, thank you very much for your continued efforts in this field.

I want to say up front, I need to go from here to the export regime hearing in the Banking Committee, where we have Messrs. Cox and Dicks. So I apologize for not being able to stay throughout this, but my staff will.

Let me begin by saying that last session the Commerce Committee became the first Senate committee to forge a consensus on this question of some kind, at least, and to report out comprehensive legislation. I am glad we are back here now and it is my hope that we can make real progress this year to develop a sensible encryption framework for the 21st century.

We have been part of this debate for some time now. I serve on the Intelligence Committee, the Foreign Relations Committee, this committee, and the Banking Committee, all of which touch on it one way or the other. I am a former prosecutor, so I have been particularly sensitive to some of the warrant issues, eavesdropping issues, intelligence-gathering issues, and so forth.

For the past several years, frankly, we have received relatively conflicting information from various interests in the debate, and I think, to our frustration, at least to my frustration, Mr. Chairman, we have been primarily debating the current state of export markets. We have debated whether there is a mature market abroad

for export products and whether we can use regulatory controls to shape that market.

I have adopted a relatively cautious approach, for a lot of very obvious reasons. I am sensitive to our national security needs and I have been very hopeful that the long and many discussions of the White House and various entities on this would retard the spread of encryption and actually shape market demand abroad.

I have a change of mind at this point and I want to express that. I think it is time to reframe the debate on encryption. As time goes on and availability abroad of strong encryption products continues to grow, it becomes more and more difficult to accept that we alone can control the development of this marketplace. If we cannot shape the development of the marketplace and have not been able to reach an adequate consensus in this country to do so in the last few years, then we are forced to a point in time, which I think we are at now, where we have to examine in a responsible way how to adjust our regulatory regime.

For a long time we have been debating, Mr. Chairman, whether to relax export controls to permit the export of stronger encryption products. I think that question has to change. It is now time to discuss how we go about creating a new scheme that recognizes the realities of the new marketplace.

I ask unanimous consent that an article from today's New York Times, "Encryption Products Found to Grow in Foreign Markets" by John Markoff, be made part of the committee record.

Senator BURNS. Without objection.

[The material referred to follows:]

THE NEW YORK TIMES

ENCRYPTION PRODUCTS FOUND TO GROW IN FOREIGN MARKETS

BY JOHN MARKOFF

Commercial data-scrambling technology that is made outside the United States has become significantly more available in the last 18 months, according to researchers at George Washington University.

The researchers' report, which is to be presented today in testimony before the Senate Commerce Committee, is part of a growing body of evidence suggesting that the Government's efforts to restrict the spread of "strong encryption" technology for secret electronic communications have largely failed.

"The Government must acknowledge that there are foreign produces, and it must concede that they are of comparable quality to U.S. technology," said Bruce Heiman, legislative counsel for Americans for Computer Privacy, the Washington-based computer industry lobbying group that financed the study.

The Government has long imposed export curbs on encryption tecnologies, invoking national security and crime prevention concerns. Officials have argued that scrambled messages would improve the ability of terrorists and other criminals to organize and plan illegal operations.

The new data, though, indicate that 805 encryption products are now available in 35 countries outside the United States—a 22 percent increase since December 1997. Moreover, 167 products are based on encryption algorithms considered too strong to be cracked by even the most powerful computers.

"In addition to the absolute increase in the number of products, we've also found that six new countries have companies that are now selling encryption technology," said Lance Hoffman, director of the Cyberspace Policy Institute at George Washington University.

He pointed to companies like Cybernetica in Estonia that use the United States export restrictions as a marketing tool.

"Cybernetica advertises: 'Strong crypto. Long keys. No export restrictions,'" he said.

The report also asserts that the United States has lost its monopoly on the basic mathematical technologies underlying data encryption.

For example, of the 15 algorithms now being considered by the National Institute of Standards for a new American encryption standard, 10 have been developed outside the United States.

The report does not offer evidence of actual use of encryption systems abroad. But Mr. Hoffman said researchers had compiled material suggesting that the most powerful encryption software was now readily accessible internationally.

"I'm holding in my hands a computer magazine we found on a French newsstand," he said in a phone interview yesterday. The publication, Magazine Dot Net, contained a CD-ROM with encryption programs including Pretty Good Privacy and a program called Scramdisk that features advanced encryption algorithms like DES, Triple DES, Blowfish and Idea—any of which would present formidable challenges to code breakers in the Federal Government.

http://www.nytimes.com

Senator KERRY. Let me just share very quickly. The new data indicates that 805 encryption products are now available in 35 countries outside the United States, a 22 percent increase since December 1997. Moreover, 167 products are based on encryption algorithms considered too strong to be cracked by even the most powerful computers. In addition to the absolute increase in the number of products, we have also found that six new countries have companies that are now selling encryption technology.

One of them, Cybernetica in Estonia, uses the U.S. export restrictions as a marketing tool: "Cybernetica advertises 'Strong crypto, long keys, no export restrictions.'" The article goes on, Mr. Chairman.

I am pleased to join Chairman McCain as an original co-sponsor of the PROTECT Act of 1999. The bill is an important first step that recognizes that as the Internet becomes more of a presence in global commerce there have to be guarantees and assurances that business and personal information remains confidential.

We have to also continue to recognize that U.S. companies are leaders in creating encryption technology and these companies are integral to our economy. We are debating a great deal now about the impact of China stealing secrets and where the long-term relationship may go. Mr. Chairman, I am persuaded, as I have been for several years, but I think for some time we have held out hope about our ability to control and shape the market. I am persuaded that the national security interest of the country is not only affected by the sort of law enforcement/security side of this, but it is also affected by the long-term economic side of it.

It seems to me that it is important for U.S. technology to be out there, for people to be using it, and that there are certain security values inherent in that happening.

The U.S. information technology companies have been deeply frustrated by what they perceive as excessive stringent controls on the export of their encryption products. Although the United States is the leader in producing high quality strong encryption products, other countries are increasingly doing so. We have to recognize that reality and understand that export controls are not going to stop the spread of encrypted products and, importantly, controls that do not recognize this reality put our software industry at a disadvantage as it tries to compete in the global marketplace and has the potential to put our security at risk.

Encryption is essential to hundreds of billions of dollars of e-commerce. It is crucial to electronically transferred funds and to overall use of the Internet, including e-mail, and the United States must have a powerful presence in that future development.

So I am open to arguments regarding whether we expand them even further than the PROTECT Act, but I believe that is an important first step and I am hopeful we can find a responsible approach that would allow us to balance some of the other interests.

I would simply ask witnesses to perhaps—I am sure they will be asked this and address it: What happens with respect to foreign companies filling the gap and what the relationship of that is to our national security if foreign encryption is produced worldwide and we are outside of that loop?; and also whether it makes sense for our policy to work in a way that is increasingly putting the United States' interests within the field of commerce at a disadvantage.

Also, there are other articles regarding other types, the Quantum code and other approaches to encryption, which raise a whole lot of issues about where we may be heading in the long run here and what we can control in terms of the market.

So Mr. Chairman, I think we are at a very important juncture and I thank you for having this hearing today and proceeding forward.

Senator BURNS. Thank you. We always like conversions.

Senator KERRY. Beware of the convert. The zeal of the convert is always the worst.

Senator BURNS. I know.

Senator, I appreciate your words today and I think as far back as 1994 and 1995, where we had security questions.

Before I recognize Senator Ashcroft, I want to make it pretty clear that we should be as policymakers giving our security people the funds and resources that their technology can stay maybe a quarter step ahead of the technology that is generally accepted around the world. I think there we have fallen down a little bit.

But I think our security people can do the job that they are paid to do and do a great job of it, but we have got to give them the funds in order for them to adapt, to go into new technology, because Moore's Law has taken over here. Our technology is going to go. We have got to make sure that we take care of our security people and they can stay with it. That is where we should be focusing our attention, I think.

Senator ASHCROFT.

STATEMENT OF HON. JOHN ASHCROFT, U.S. SENATOR FROM MISSOURI

Senator ASHCROFT. Thank you, Mr. Chairman. I want to thank the Senator from Montana for his leadership in this area. Leadership is not finding out where people already are and going and standing at the front of the line. Leadership is finding out where we need to go and helping people understand how to get there, and certainly you have done that, especially as it relates to this issue.

I want to thank the chairman of this committee for having this hearing today to address an issue that I believe is central to the future of our country's ability to remain a worldwide leader in elec-

tronic technology. That is the development and the availability of data encryption technology.

Encryption of sensitive electronic data is essential to our modern economy. State and national infrastructures, financial transactions, and of course the burgeoning field of Internet commerce all depend on the ability of companies, institutions, and individuals to securely transmit electronic data, and American products are at the forefront of this industry.

I might add that if American products are not at the forefront of this industry, other products will be at the forefront of this industry.

For years now, since before I first came to the Capitol, American manufacturers of encryption technology have been hamstrung in their efforts to compete in the global marketplace regarding these products by export controls that reflect a complete misunderstanding of the incredibly dynamic and fluid nature of encryption technology. We have tried for over 4 years to remedy that situation.

I first introduced the E-PRIVACY bill in the last Congress and intend to reintroduce it shortly in this Congress. But unfortunately, nothing has been accomplished by way of assistance to law enforcement and to industry or, most importantly, to the users of encryption in this country.

Unfortunately, a significant barrier to progress on this issue has been the Administration, which has taken an active and open position against permitting the export of encryption technology and indeed a fairly hostile view to the unregulated domestic use of encryption. The Administration bases its position on the grounds that robust encryption allegedly presents risks to law enforcement and national security, a view that I think will be shown to be mistaken by today's testimony. We certainly have endured national security risks, but it has not been from the industry's development of encryption.

In addition, there has not always been agreement here in Congress about the need to free our technology industry from these export restrictions. I am happy to note that this appears to have changed. The chairman's PROTECT Act which we are here to discuss, demonstrates that there is a growing consensus that the Administration is mistaken and that deregulation of encryption is necessary in order for us to maintain our leadership position in this industry, and I want to commend the chairman for helping us to build that consensus.

I think that the PROTECT Act is a big step in the right direction on encryption. In fact, it shares many of the same principles and provisions included in my E-PRIVACY bill. However, I do think that the PROTECT Act needs to go further in two ways.

First, the PROTECT Act needs to reflect the lightning-fast nature of development in this industry and institute export relief that will not make the products eligible for decontrol obsolete by the time the approval process is complete. The Administration has long taken the route of regulating encryption exports based on the bit length of the product, with little regard to the current state of the technology. It began with permitting the export of 40-bit technology 7 years ago and only agreed last fall to increase the limit to 56-bit technology. Of course, the standard for generally available prod-

ucts worldwide is already 128-bit technology. That is where the competition is. So the Administration's position is already sorely outdated.

In fact, months ago I came to a meeting of this committee with an advertisement from the Internet which was from the Siemens company in Germany advertising robust 128-bit encryption, saying that you cannot get this from a U.S. manufacturer, at least someone overseas could not. The advertisement also indicated, however, that if you buy this you can use it in the United States and you can use it overseas as well. So if you want to have robust encryption, buy it from the Germans, from Siemens.

The Administration has decided to tie the hands of the U.S. encryption industry. To me that is a disaster. But it is also compounded by people beginning to develop relationships with foreign software providers as a result of the unavailability of 128-bit or robust encryption on the part of U.S. providers of software.

To see the Germans eagerly promoting this potential and to have people from my own State of Missouri say to me, "John, we have an office in Singapore"—this happened to me—we have not been able to speak with them confidentially and communicate with them and the government is making it impossible for us to send the encryption that we can use domestically. We cannot send it to our office in Singapore because we are ineligible to export it.

I do not want that situation to be—well, I just do not want the situation to be such that I have to say, "Well, go to Siemens in Germany, from Siemens you can buy the encryption that can be sent into the United States and from Siemens in Germany it can be sent to Singapore, so you can have your cake and eat it, too, by dealing with a non-domestic firm."

For us to have a policy which provides for the slitting of our own throats in a technology arena that is developing at a rapid pace is simply unwise. I think it is foolhardy. If we are to mark the next century as an American century, or even to celebrate the next week as high technology week in the Senate, we must be forward-thinking and acting.

The PROTECT Act deregulates products up to 64 bits. That is a good start. The problem is that the Act delays general decontrol of 128-bit technology until 2002, by which time it will almost certainly be as obsolete as 56-bit encryption is today. In the interim, PROTECT permits individual exceptions for higher bit technology export, but it creates a regulatory approval board and a process that can take up to 60 days to determine whether a product is already generally available, something that, quite frankly, can be determined by surfing the Internet for a little while, I mean moments.

With all due respect, this process is too long, which is why in the E-PRIVACY bill we give the administration a one-time 15-day review of products that are generally available before they are permitted to export them.

I urge my colleagues to press our panelists on the second panel for answers on whether they can remain competitive if we wait as long as the PROTECT Act provides.

The second area where I think the PROTECT Act can go farther is the explicit delineation of the rights and procedural protections

of Americans in their ability to use encryption and to be secure in their use of encrypted data. While the PROTECT Act clearly affirms this right, it is relatively silent on the balance of procedural protections between Americans' privacy interests and legitimate law enforcement efforts. I do not think we can afford to be silent on this issue.

The administration and the FBI have over time indicated support for language that would mandate key recovery for all domestic encryption and alternatively support several suggested approaches that would make using domestic key escrow a practical, although not legal, necessity. Director Freeh has gone so far as to mention the need for a new fourth amendment that considers the "realities" of the digital age.

I think we need a new and improved approach to domestic encryption, not a new updated version of the fourth amendment, and I for one am not eagerly awaiting the FBI's new release of the fourth amendment 2.0 or first amendment 98. I am, however, eager to hear what the Administration's current position is on key recovery and key escrow.

My own E-PRIVACY bill sets out specific procedures for balancing the legitimate interests of law enforcement with the privacy rights of Americans, and I hope that any final legislation passed by the Senate would include such provisions. Those are my two observations.

Again, I want to say that the PROTECT Act is a strong step in the right direction toward protecting American privacy rights and American industry, but I think it should go further.

I look forward to hearing from our panelists today and engaging them in serious discussion on these issues, and I thank the gentleman from Montana, whose leadership in this area has been very valuable to America.

Senator BURNS. Thank you very much, Senator. It has been an issue that both of us have been around a day or two, so we are not complete strangers to it.

Congressman Goodlatte is on his way. In the meantime—oh, he is here.

Mr. GOODLATTE. Hiding.

Senator BURNS. You are still on your way, right?

Senator ASHCROFT. On his way to the microphone.

Senator BURNS. That is right, that is right.

Congressman, we thank you. You have been a great leader on this issue in the House and we appreciate your coming over this morning and offering your thoughts on this piece of legislation.

STATEMENT OF HON. BOB GOODLATTE, U.S. REPRESENTATIVE FROM THE STATE OF VIRGINIA

Mr. GOODLATTE. Well, Senator, thank you for the opportunity to testify before the Senate Commerce Committee today. I want to commend you and Chairman McCain and Senator Ashcroft for your hard work in this area. I was delighted to hear the comments of Senator Kerry a little while ago. I had brought the same New York Times article with me, so I will not need to ask that it be made part of the record.

But I do want to point out that one of the items in here that he did not mention is that the United States has lost its monopoly on the basic mathematical technologies underlying data encryption. For example, of the 15 algorithms now being considered by the National Institute of Standards for a new American Encryption Standard, 10 have been developed outside of the United States. If we do not act on this soon, we are going to be left behind in that regard.

I also would ask that the committee consider making part of the record an article by Congressman Chris Cox, who is, as you know, the chairman of the committee that just released the Cox report and who is a strong supporter of changes in our export controls laws related to encryption and a co-sponsor of our legislation in the House, the SAFE Act. He has an article that was published in the San Jose Mercury News entitled "China: Export of Technology Would be Liberating Force." I think it makes a very strong case for why, while export controls are appropriate in some sectors, liberalizing our export controls on encryption would be of great benefit to our nations.

Senator BURNS. That will be made part of the record.

[The material referred to follows:]

CHINA: EXPORT OF TECHNOLOGY WOULD BE LIBERATING FORCE

(By Christopher Cox)

American Policy toward the People's Republic of China should proceed from this central premise: It is our sincere hope for the Chinese people that they will no longer live under a communist government.

To this end, America's—and California's—world leadership in high-tech enterprise promises far more than economic benefits. The export of these products to the Chinese people can be a great democratizing and liberating force.

In January, the People's Republic sentenced Lin Hai, a 30-year-old software executive and Web page designer, to prison for supposedly "inciting subversion of state power." His so-called "crime" consisted of exchanging e-mail addresses with an anti-communist group in America.

But if Lin Hai had been able to keep the contents of his computer messages away from the prying eyes of the Ministry of State Security—using strong encryption in commercially available software—he would be a free man today.

That is why America's companies, the leaders in encryption technology, must be able to export their products to China and around the world.

Strong encryption is—as Beijing's communist leadership is well aware—a massive threat to totalitarian regimes and their government-maintained monopoly on information, because it permits individuals to communicate privately without fear of government eavesdropping or interception.

In this and the previous Congress, I have sponsored the Security and Freedom through Encryption Act, together with a broad coalition of Republican and Democratic lawmakers, I disagree with the Clinton-Gore administration, and with Sen. Dianne Feinstein, that the current prohibition on American businesses exporting encryption software is necessary for our national security.

Yet the Clinton-Gore administration would go beyond the current prohibition, endorsing not just restrictions on encryption exports, but also requiring every encryption program sold—even within the United States—to have a secret key to permit eavesdropping by law enforcement officials or foreign governments.

The Clinton-Gore administration seems to place a higher priority on stopping the export of encryption software to the Chinese people than on preventing the theft of our nuclear weapons technology by the People's Liberation Army.

This is exactly backward. Rather than control commercially available computers, software and technology, we should safeguard our most critical military secrets.

TRANSFER OF TECHNOLOGY

For the past nine months, I've chaired a congressional select committee investigating the transfer of militarily sensitive technology to the People's Republic of China. The committee's classified report, unanimously approved by all five Repub-

licans and four Democrats, found overwhelming evidence that such transfers—including theft through espionage—have caused serious harm to U.S. national security, and continue to this day.

But some have inferred that this should mean clamping down on commercial exports. To the contrary: The committee found that the current export-licensing process is riddled with errors and plagued by delays. It often does very little to protect our national security—while frequently doing a great deal to damage America's competitiveness in world markets.

The committee has therefore recommended streamlining export rules. The United States should provide a new "fast track" for most items, while focusing greater resources and expertise on the limited targets that we know from our intelligence are the subject of specific collection efforts by the People's Republic of China and others.

Trade in innovative technologies, goods and services can help undermine inefficient state-run industries and bring hope of a better life to the Chinese people.

In areas like transportation, telecommunications and financial services, it is the means by which communist China—whose economy is smaller on a per capita basis than Guatemala's—can become a developed nation.

In fields such as medicine, biotechnology and farming, U.S. trade offers hope for the desperately poor millions who are still China's majority that they will be able to each and survive.

Encouraging exports to China that promote individual freedom and well-being is in the United States' national security interest. For this reason, in addition to allowing the export of encryption software, U.S. policy should focus on unleashing the Internet as an engine of freedom in China.

Among the 1.2 billion people in the People's Republic of China, only one in a thousand is an Internet user. But Internet use is growing at a rate that threatens the Communist Party's grip on China.

As Chinese journalist Sang Ye has observed: "New ways of thinking, of communicating, of organizing people and information—the Net takes aim squarely at things that since Mao's earliest days have been the state's exclusive domain."

Today's China's communist dictatorship is working hard to re-route its citizens away from the information superhighway and onto the state-controlled "Intranet." This new Intranet allows communication only among approved users who share communist-approved content. The Ministry of Post and Telecommunications supervises and approves all networks, and its screens virtually all news and even financial information that citizens may receive from foreign sources.

While the Chinese Communist Party argues, on the Internet home page of the People's Daily, that the open flow of communications would be destabilizing, Americans know from our own experience that technology is best used as a means to an end: a promise of greater freedom.

The United States should move aggressively to frustrate the Chinese government's censorship of the Internet by condemning it as a barrier to free trade, an impediment to joining the World Trade Organization, and a violation of the several human rights covenants it has signed. And we should encourage the construction of an expanded Internet architecture that frustrates censorship and control by repressive states.

At the same time, the United States should work with all nations for the establishment of the Internet as a global free-trade zone, which not only will make it increasingly difficult for governments including China's to choke off access but also will pressure them further to reduce protectionist trade barriers.

Finally, we should recognize that while our currently limited trade with China's protectionist government may be better than nothing, the object of U.S. policy must be a liberalization of trade that is fundamentally at odds with the nation's communist system.

TRULY FREE TRADE

Despite America's free-trade policy, we still sell less to the billion-plus People's Republic of China than to the 22 million people of Taiwan. Instead of business ventures being approved one at a time by the Communist Party's Politburo, truly free trade means a billion Chinese interacting independently with a quarter-billion Americans.

A policy toward the People's Republic of China that frustrates this objective is both shortsighted and cruel.

The recent public attention to espionage raises proper concerns about our lack of security, but it should not distract us from our objective of freedom for China's people—a result that American technology exports can help bring about.

Today, we have the worst of both worlds: Military technology that the communist government can use to hold the Chinese people in terror is being stolen, while commercial technology that can liberate the Chinese people is delayed in the export-licensing bureaucracy.

It's time to focus not on whether to engage—we should all be agreed on that—but rather on the terms of engagement. We should have no illusions about with whom we are dealing. We should have no doubt about where our policy is taking us. Freedom—not engagement and possibly marriage to a communist dictatorship—is what our policy toward China should be seeking to achieve. *U.S. Rep. Christopher Cox, R-Newport Beach, is chair of the House Select Committee on U.S. National Security and Military-Commercial Concerns with the People's Republic of China. He wrote this article for the San Jose Mercury News Sunday Perspective section.*

Mr. GOODLATTE. Thank you, Mr. Chairman.

As you know, I have worked for many years on the encryption issue in the House. The legislation I have introduced in this Congress, H.R. 850, the Security and Freedom Through Encryption Act of 1999, currently has 257 co-sponsors, including a majority of both the Republicans and Democrats in the House and a majority of both the Republican and Democratic leadership.

The SAFE Act has passed the House Judiciary Committee by voice vote and is now pending before the Committees on International Relations, Commerce, Armed Services, and Intelligence. Each of these additional committees is expected to act soon on the legislation and it is my hope that the SAFE Act will be considered by the House in the summer or early fall.

Encryption has many benefits. First, it aids law enforcement by preventing piracy and white collar crime on the Internet. Several studies over the past few years have demonstrated that the theft of proprietary business information costs American industry hundreds of billions of dollars each year. The use of strong encryption to protect financial transactions and information would prevent this theft from occurring.

With the speed of transactions and communications on the Internet, law enforcement cannot stop thieves and criminal hackers by waiting to react until after the fact. Only by allowing the use of strong encryption, not only domestically but internationally as well, can we hope to make the Internet a safe and secure environment.

As the National Research Council's Committee on National Cryptography Policy concluded:

If cryptography can protect the trade secrets and proprietary information of businesses and thereby reduce economic espionage, which it can, it also supports in a most important manner the job of law enforcement. If cryptography can help protect nationally critical information systems and networks against unauthorized penetration, which it can, it also supports the national security of the United States.

Second, if the global information infrastructure is to reach its true potential, citizens and companies alike must have the confidence that their communications and transactions will be secure.

Third, with the availability of strong encryption overseas and on the Internet, the Administration's export restrictions only serve to tie the hands of American business. Due in large part to these export controls, foreign companies are winning an increasing number of contracts by telling prospective clients that American encryption products are weak and inferior, which is robbing our economy of jobs and revenue. I understand you are going to hear testimony further in regard to the new report mentioned in the New York Times article, which Senator Kerry made a part of the record.

In fact, one study, one noted study, found that failure to address the current export restrictions by the year 2000 will cost American industry $60 billion and 200,000 jobs. Under the current system, America is surrendering our dominance of the global marketplace.

The SAFE Act remedies this situation by allowing the export of generally available American-made encryption products after a 15-day, one-time technical review. Additionally, the bill allows custom-designed encryption products to be exported after the same review period if they are commercially available overseas and will not be used for military or terrorist purposes.

The SAFE Act enjoys the support of members, individuals, and organizations across the entire spectrum of ideological and political beliefs, not only because it is a common sense approach to solving a serious problem, but also because ordinary Americans' privacy and security is being assaulted by this Administration.

Amazingly enough, some in the Administration want to mandate a back door into people's computer systems in order to access their private communications. In fact, some in the Administration have stated that if people do not voluntarily create this back door, they may seek legislation forcing them to give the Government access to their information by mandating a key recovery system requiring people to give the keys to decode their communications to a government-approved third party. This is the technological equivalent of mandating that the Government be given a key to every home in America.

Mr. Chairman, I would also like to note that we will hear from Administration representatives who will say that they do not support a mandatory key recovery system. One of the problems we have had in addressing this is that the Administration has not been speaking with one voice and there has been an inconsistency with regard to their policy.

I would like to note with great appreciation the position you and Chairman McCain have taken on this issue in the PROTECT Act. I could not agree more with the domestic-related provisions of your legislation which, like the SAFE Act, prevent the Administration from putting roadblocks on the information superhighway by prohibiting the Government from mandating a back door into the computer systems of private citizens and businesses.

Additionally, both the PROTECT Act and the SAFE Act ensure that all Americans have the right to choose any security system to protect their confidential information.

I would like to encourage you to consider further changes in this area with regard to export controls. Certainly the immediate decontrol of 64-bit encryption is helpful to our industry, as are the provisions allowing the export of strong encryption to, as you have called them, legitimate and responsible entities or organizations and their strategic partners, and the unlimited export of encryption once the new AES standard is developed and implemented. These are marked improvements over Chairman McCain's legislation contained in S. 909 from the last Congress.

Our industry needs export relief now and I do not believe that it can afford to wait until the AES standard is adopted a few years from now. While the immediate decontrol of 64-bit encryption is better than the Administration's current 56-bit level, the industry

standard is, as has been noted here today, 128 bits, which consumers and companies alike are demanding to protect their communications and transactions.

So as the PROTECT Act moves through the Senate, I encourage you to continue to look for ways to provide further export relief to U.S. industry.

I would also like to note that the SAFE Act does not completely eliminate export controls on encryption products. Like the PROTECT Act, the SAFE Act allows the President to prohibit encryption exports to terrorist states and impose embargoes and allows the Secretary of Commerce to stop the export of specific products to specific individuals or organizations in specific countries if there is substantial evidence that they will be used for military or terrorist purposes.

As NSA Deputy Director Barbara McNamara recently testified before the House Commerce Committee, "end uses and end users are what the Administration uses to determine whether a product should be exported. This is official government policy." With the millions of communications, transmissions, and transactions that occur on the Internet every day, American citizens and businesses must have the confidence that their private information and communications are safe and secure.

I want to again thank you for allowing me to testify today and I look forward to working with you and Senator Ashcroft as you move forward on this legislation. We hope you can pass a good bill out of the Senate. We will try to do the same thing in the House and work together to resolve this problem.

Thank you.

[The prepared statement of Representative Goodlatte follows:]

PREPARED STATEMENT OF HON. BOB GOODLATTE, U.S. REPRESENTATIVE FROM VIRGINIA

Mr. Chairman, I would like to thank you for inviting me to testify today on legislation you have introduced—S. 798, the PROTECT Act of 1999—to encourage the use of strong encryption.

As you know, I have worked for many years on the encryption issue in the House. The legislation I have introduced this Congress, H.R. 850, the Security And Freedom through Encryption (SAFE) Act of 1999, currently has 257 cosponsors, including a majority of both the Republican and Democratic leadership. The SAFE Act has passed the House Judiciary Committee by voice vote, and is now pending before the committees on International Relations, Commerce, Armed Services, and Intelligence. Each of these additional committees is expected to act soon on the legislation, and it is my hope that the SAFE Act will be considered by the House in the summer or early fall.

Encryption has many benefits. First, it aids law enforcement by preventing piracy and white-collar crime on the Internet. Several studies over the past few years have demonstrated that the theft of proprietary business information costs American industry hundreds of billions of dollars each year. The use of strong encryption to protect financial transactions and information would prevent this theft from occurring. With the speed of transactions and communications on the Internet, law enforcement cannot stop thieves and criminal hackers by waiting to react until after the fact.

Only by allowing the use of strong encryption, not only domestically but internationally as well, can we hope to make the Internet a safe and secure environment. As the National Research Council's Committee on National Cryptography Policy concluded, "If cryptography can protect the trade secrets and proprietary information of businesses and thereby reduce economic espionage (which it can), it also supports in a most important manner the job of law enforcement. If cryptography can help protect nationally critical information systems and networks against unauthor-

ized penetration (which it can), it also supports the national security of the United States."

Second, if the Global Information Infrastructure is to reach its true potential, citizens and companies alike must have the confidence that their communications and transactions will be secure.

Third, with the availability of strong encryption overseas and on the Internet, the Administration's export restrictions only serve to tie the hands of American business. Due in large part to these export controls, foreign companies are winning an increasing number of contracts by telling prospective clients that American encryption products are weak and inferior, which is robbing our economy of jobs and revenue. In fact, one noted study found that failure to address the current export restrictions by the year 2000 will cost American industry $60 billion and 200,000 jobs. Under the current system, America is surrendering our dominance of the global marketplace.

The SAFE Act remedies this situation by allowing the export of generally available American-made encryption products after a 15-day, one-time technical review. Additionally, the bill allows custom-designed encryption products to be exported, after the same review period, if they are commercially available overseas and will not be used for military or terrorist purposes.

The SAFE Act enjoys the support of members, individuals and organizations across the entire spectrum of ideological and political beliefs, not only because it is a common-sense approach to solving a serious problem, but also because ordinary Americans' privacy and security is being assaulted by this Administration.

Amazingly enough, the Administration wants to mandate a back door into peoples' computer systems in order to access their private communications. In fact, the Administration has stated that if people do not "voluntarily" create this back door, it may seek legislation forcing them to give the government access to their information, by mandating a "key recovery" system requiring people to give the keys to decode their communications to a government-approved third party. This is the technological equivalent of mandating that the government be given a key to every home in America.

Mr. Chairman, I would like to note with great appreciation the position you have taken on this issue in the PROTECT Act. I couldn't agree more with the domestic-related provisions of your legislation, which—like the SAFE Act—prevent the Administration from placing roadblocks on the information superhighway by prohibiting the government from mandating a back door into the computer systems of private citizens and businesses. Additionally, both the PROTECT Act and the SAFE Act ensure that all Americans have the right to choose any security system to protect their confidential information.

On the issue of export relief, I would also like to commend you for the changes you have made in this year's bill. Certainly the immediate decontrol of 64-bit encryption is helpful to our industry, as are the provisions allowing the export of stronger encryption to, as you have called them, "legitimate and responsible entities or organizations and their strategic partners," and the unlimited export of encryption once the new AES standard is developed and implemented. These are marked improvements over the export restrictions contained in S. 909 from the last Congress.

However, I would like to encourage you to consider further changes in this area, along the lines of those contained in the SAFE Act. Our industry needs export relief now—I do not believe that it can afford to wait until the AES standard is adopted a few years from now. And while the immediate decontrol of 64-bit encryption is better than the Administration's current 56-bit level, the industry standard is currently 128-bit encryption—which consumers and companies alike are demanding to protect their communications and transactions. So as the PROTECT Act moves through the Senate, I encourage you to continue to look for ways to provide further export relief to U.S. industry.

I would also like to note that the SAFE Act does not completely eliminate export controls on encryption products. Like the PROTECT Act, the SAFE Act allows the President to prohibit encryption exports to terrorist states and impose embargoes, and allows the Secretary of Commerce to stop the export of specific products to specific individuals or organizations in specific countries if there is substantial evidence that they will be used for military or terrorist purposes. And as NSA Deputy Director Barbara McNamara recently testified before the House Commerce Committee, "end uses and end users are what we use to determine whether a product should be exported—this is official government policy."

With the millions of communications, transmissions, and transactions that occur on the Internet every day, American citizens and businesses must have the confidence that their private information and communications are safe and secure.

Again, thank you for allowing me to testify today, and I look forward to working together with you as the PROTECT Act moves through the Senate and the SAFE Act moves through the House.

Senator BURNS. Thank you very much, Congressman. We appreciate your interest and leadership in this issue.

I am going to call the panel. Any questions for the Congressman?

Senator ASHCROFT. May I just commend the Congressman. I have had the opportunity and good fortune to work with him, and his understanding of the issues related to encryption is unsurpassed in the Congress. I appreciate that, and I think, frankly, the American people and the data industry owes you a debt of gratitude. I know that I do, and I thank you for your leadership.

Mr. GOODLATTE. Thank you for your kind words.

Senator SNOWE. Mr. Chairman.

Senator BURNS. The Senator from Maine.

STATEMENT OF HON. OLYMPIA J. SNOWE, U.S. SENATOR FROM MAINE

Senator SNOWE. Thank you, Mr. Chairman. I want to welcome my good friend and former colleague from the House here today, and commend you for your leadership on this issue and your presentation before the committee.

Mr. GOODLATTE. Thank you, Senator Snowe. I would like to tell you that I will be in your State, in fact in your home town, tomorrow and Saturday for my 25th reunion at Bates College. So I appreciate your kind words.

Senator SNOWE. I wish you good weather and great lobsters.

Mr. GOODLATTE. Thank you.

Senator BURNS. At least they have got a warning up there, right?

Mr. GOODLATTE. That is right.

Senator BURNS. We like these warnings.

I will call the first panel to the table, and while they are coming up, Senator Snowe, do you have a statement that you would like to make?

Senator SNOWE. No, Mr. Chairman. I have a statement for the record.

Senator BURNS. It will be made part of the record.

[The prepared statement of Senator Snowe follows:]

PREPARED STATEMENT OF HON. OLYMPIA J. SNOWE, U.S. SENATOR FROM MAINE

Thank you, Mr. Chairman. Today's hearing is extremely important because it addresses an issue that will only grow in importance as the Global Information Infrastructure (GII) continues to develop and evolve: the availability of strong encryption technology.

Without the knowledge that one's information is private and secure, the full potential of the Global Information Infrastructure—and the transmission and utilization of information on the Internet in particular—will never be realized.

On the one hand, if one is certain that their proprietary or personal information can only be accessed by those for whom it is intended, one will be at ease putting business plans, personal medical records, and other confidential files "on-line". But if security is inadequate for the prevention of unauthorized "browsing" or outright "piracy," one's willingness to utilize the countless benefits of on-line commerce will be severely hampered.

The United States imposes limits on the export of encrypted products— in part— to ensure that law enforcement and intelligence agencies have easier access to the information these products contain. Presumably, if the products exported by the United States do not allow for encryption beyond a certain level, the threat to national security will be lessened.

While I believe we would all agree that national security is of the utmost importance—and any policy that protects American citizens from "on-line crime" is beneficial—it is also important that we be realistic in setting these policies. If our policies do not reflect the reality of the global marketplace, we will not only fail to accomplish the goals we are pursuing, but we may also risk harming businesses and consumers in the United States that we are seeking to protect.

In addition, high-tech industries in the United States have a great deal at stake in the ongoing debate on encryption export restrictions. If our current export policies are "behind the times," domestic producers of computer hardware and software risk being at a competitive disadvantage in the global marketplace. At the same time, other U.S. companies that rely on the use of these encrypted technologies to manufacture consumer products—such as cellular telephones—could also be adversely impacted by a poorly conceived export policy.

Accordingly, today's hearing will give us a chance to review the need for, and impact of, S. 798, the PROTECT Act—legislation that would fundamentally alter the manner in which encryption export restrictions are established. Ultimately, it is my hope that this hearing will assist us in determining whether or not our current export restrictions are both practical and effective, and if changes such as those contained in S. 798 would be a step forward or a step back for the United States.

I would like to thank our witnesses for being with us this morning, and look forward to the discussion this hearing will generate on a topic that is so fundamental to the development of the world's information infrastructure. Thank you, Mr. Chairman.

Senator BURNS. We have William Reinsch, who is the Under Secretary of Export Administration, Department of Commerce; James Robinson, Assistant Attorney General from the Criminal Division; and we have Barbara McNamara, Deputy Director of the National Security Agency.

We appreciate all of you taking time in your busy days and your responsibilities and duties to come and visit with us today about this very important subject. We will just go in order, I guess. So Secretary Reinsch, we look forward to hearing from you and some of yours.

I might add that your complete statement will be made part of the record. If you want to consolidate that and offer your views, that is perfectly OK, too. We appreciate you coming today.

Mr. Secretary, good to see you again.

STATEMENT OF HON. WILLIAM A. REINSCH, UNDER SECRETARY OF EXPORT ADMINISTRATION, U.S. DEPARTMENT OF COMMERCE

Mr. REINSCH. Thank you, Mr. Chairman. It is good to be back. I do have a shorter statement. We have a lot to say about this bill, however, so it is not quite as short as it could be, I suppose.

I want to thank you for the opportunity to be back to discuss this difficult subject. I think we made a lot of progress since I was here the last time, and that is one of the subjects I want to discuss with you.

It should be obvious from the testimony today that encryption is a hotly debated issue. I want to make clear what the Administration's policy is. We support a balanced approach which considers privacy and commerce, as well as protecting important law enforcement and national security equities. We have been consulting closely with industry and its customers to develop a policy that provides that balance in a way that also reflects the evolving realities of the marketplace.

There is no question about the evolving role of encryption in the marketplace and in e-commerce, and my full statement has a lot

to say about that in terms of details, I will not pass that on to this committee at this time because you are already well familiar with it.

But I do want to say that developing a balanced policy is complicated because we do not want to hinder encryption's legitimate use, but at the same time we do want to protect national security and law enforcement. Now, over the last several years as we have been studying this problem we have learned that there are many ways to assist lawful access beyond key escrow or key recovery and that there is no one-size-fits-all solution. We believe our policy reflects that, and I would like to describe it for you.

We published a regulation in September 1998, which allows the export of unlimited strength encryption to banks and financial institutions. This allows U.S. companies new opportunities to sell encryption products to a key market for encryption products.

Last September, the Vice President also unveiled an update to our policy, and we published regulations implementing it last December. It permits the free export of unlimited strength encryption products to several key sectors of the market. In addition to banks and financial institutions, we now allow health facilities and online merchants to purchase U.S. encryption to secure their sensitive financial, medical, and online transactions in digital form. U.S. companies can now export 128-bit or greater encryption products, including encryption technology, to subsidiaries located worldwide to protect proprietary information and to develop new products.

Furthermore, this update allows the export of unlimited strength recovery-capable or recoverable products. These products do not require a third party to hold any key, are not key escrow, but allow for law enforcement access under proper court authority. They are readily available in the marketplace and include general purpose routers, firewalls, and virtual private networks.

We have also made progress with other countries, Mr. Chairman, through the hard work of Ambassador David Aaron, the President's Special Envoy on Cryptography. We agreed in the Wassenaar arrangement last December on several changes relating to encryption controls. We removed multilateral controls on all encryption products at or below 56 bits and certain consumer items regardless of key length.

We also agreed to amend the General Software Note on this issue. Drafted in 1991 when banks, governments, and militaries were the primary users of encryption, the General Software Note did not give countries the legal authority to require a license for the export of mass market encryption software. The note was created to release general purpose software used on PCs, but it inadvertently also released encryption.

We believed it was essential to modernize the note and close the loophole. Under a new Cryptography Note adopted in December, a 64-bit key length threshold has been set for mass market encryption software and hardware. This enables governments to review export mass market products stronger than 64 bits.

I want to be clear. This does not mean that encryption products of more than 64 bits cannot be exported. Our own policy permits that, as I just made clear, as does the policy of most other Wassenaar members. It does mean the products must be reviewed

by governments consistent with their national policies before export.

Now, let me comment in conclusion, Mr. Chairman, on the PROTECT Act. With respect to S. 798, the Administration opposes this legislation for a number of reasons. Overall, we believe it does not promote the balance that we worked so hard to achieve over the last several years and which I have just defined.

Let me discuss several, but not all, of the more problematic sections. Under section 505, the removal of export controls on publicly or generally available encryption is left to an advisory board. We believe such a board would be unworkable. The broad definitions used in the bill would give the board wide latitude in making its findings on what is available. This could place the Secretary in the position of having to routinely object to the removal of export controls when important national security and law enforcement interests are at stake.

The bill also makes this decision subject to judicial review. The Administration does not think it is wise public policy for the courts to adjudicate executive branch decisions on national security matters like the ones that would be rolled into these kinds of decisions.

Section 501 of the bill removes the Department of Justice from the encryption export license consultation process. Since law enforcement interests are an important consideration in regard to encryption, we cannot support that provision. We do support the provisions that require a technical review for eligibility for export under a license exception. That is consistent with our current regulations. What we cannot support, however, is the portion of section 504 that would provide automatic eligibility after 15 days if there has been no decision from the government.

That same section also proposes control parameters and export liberalizations beyond what we can entertain and which would be contrary to our international export control obligations. For example, Wassenaar agreed to decontrol products up to 56 bits. This bill would decontrol products using a key length of 64 bits or less.

Section 504 also expands the products, end users, and countries eligible beyond what we are willing to consider at this point.

Section 102 is also troubling, as it would permit a U.S. person located anywhere in the world to develop, manufacture, sell or use any type of encryption. This would in effect prevent the government from requiring a license for U.S. persons to develop and manufacture encryption abroad. As a result, U.S. companies would likely move all development and manufacture of encryption out of the United States in order to take advantage of this loophole. This is not in our country's economic or national security interests.

Section 103 contains a provision that would prohibit the U.S. Government from conditioning any approval on the fact that a product is recoverable. A fundamental feature of our encryption policy is that we provide incentives for companies to develop products that provide strong security and also meet the needs of national security and law enforcement. The bill would eliminate this laudable feature of our policy that industry had asked us to include in last year's update. This provision is also inconsistent with section 504, which allows license exception treatment for recoverable products.

Now, we have also some problems, Mr. Chairman, with other non-export control provisions of the bill. Section 202 requires that encryption products used by the Government must interoperate with other commercial encryption products. The extent to which interoperability is required is unclear in the bill as drafted, but we believe that the practical result of the bill would be that the Government could not use encryption because no single encryption product interoperates with all other products.

It also appears that this provision could prohibit the use of encryption developed by the Government for its own internal use in closed systems that are purposefully designed not to interoperate with other systems, such as those used by the Department of Defense or the National Security Agency.

I want to make clear we do not seek encryption export control legislation, nor do we believe that legislation is needed. We believe the current regulatory structure is sufficient for balanced oversight. As the Senators here today know, public debate on this issue has often been lively and on some occasions acrimonious, although certainly not in this room. We hope to find a middle ground that can meet all of our needs.

Our dialog with industry has gone a long way toward bridging that gap and finding that middle ground. We will continue this policy of cooperative exchange, which is clearly the best way to pursue our policy objectives of balancing public safety, national security, and the competitive interests of our companies.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Reinsch follows:]

PREPARED STATEMENT OF WILLIAM A. REINSCH, UNDER SECRETARY FOR EXPORT ADMINISTRATION, U.S. DEPARTMENT OF COMMERCE

Thank you, Mr. Chairman, for the opportunity to testify on the direction of the Administration's encryption policy. We have made a great deal of progress since my last testimony before this Committee on this subject.

Even so, encryption remains a hotly debated issue. The Administration continues to support a balanced approach which considers privacy and commerce as well as protecting important law enforcement and national security equities. We have been consulting closely with industry and its customers to develop a policy that provides that balance in a way that also reflects the evolving realities of the market place.

One of the many uses of the Internet which will have a significant affect on our everyday lives is electronic commerce. The Internet and other digital media are becoming increasingly important to the conduct of international business. There were 43.2 million Internet hosts worldwide last January compared to only 5.8 million in January 1995. According to a recent study, the value of e-commerce transactions in 1996 was $12 million. The projected value of e-commerce in 2000 is $2.16 billion. To cite one example, travel booked on Microsoft's Website has doubled every year since 1997, going from 500,000 to an estimated 2.2 million this year. Many service industries which traditionally required face-to-face interaction such as banks, financial institutions and retail merchants are now providing cyber service. Customers can now sit at their home computers and access their banking and investment accounts or buy a winter jacket with a few strokes of their keyboard.

Furthermore, most businesses maintain their records and other proprietary information digitally. They now conduct many of their day-to-day communications and business transactions via the Internet and E-mail. An inevitable byproduct of this growth of electronic commerce is the need for strong encryption to provide the necessary secure infrastructure for digital communications, transactions and networks. The disturbing increase in computer crime and electronic espionage has made people and businesses wary of posting their private and company proprietary information on electronic networks if they believe the infrastructure may not be secure. A robust secure infrastructure can help allay these fears, and allow electronic commerce to continue its explosive growth.

Developing an encryption policy has been complicated because we do not want to hinder its legitimate use—particularly for electronic commerce; yet at the same time we want to protect our vital national security, foreign policy and law enforcement interests. We have concluded that the best way to accomplish this is to continue a balanced approach: to promote the development of strong encryption products that would allow lawful government access to plain text under carefully defined circumstances; to promote the legitimate uses of strong encryption to protect confidentiality; and continue looking for additional ways to protect important law enforcement and national security interests.

During the past three years, we have learned that there are many ways to assist lawful access. There is no one-size-fits-all solution. The plans for recovery encryption products we received from more than 60 companies showed that a number of different technical approaches to recovery exist. In licensing exports of encryption products under individual licenses, we also learned that, while some products may not meet the strict technical criteria of our regulations, they are nevertheless consistent with our policy goals.

Additionally, we decided that the use of strong non-recovery encryption within certain trusted industry sectors is an important component of our policy to protect private consumer information and allow our U.S. high-tech industry to maintain its lead in the information security market. Taking into account all that we have learned and reviewing international market trends and realities, we made several changes in 1998 to our encryption policy that I will now summarize.

In September 1998, we published a regulation allowing the export, under a license exception, of unlimited strength encryption to banks and financial institutions located in 46 countries which allows U.S. companies new opportunities to sell encryption products to the world's leading economy. This policy recognizes the need to secure our financial networks, and the history of cooperation which the banking and financial communities have with government authorities when information is required to combat financial and other crimes.

More importantly, on September 16th, Vice President Gore unveiled an update to our encryption policy. This Policy Update was the result of a dialogue with U.S. industry, law enforcement, and privacy groups on how our policy might be improved to find technical solutions, in addition to key recovery, that can assist law enforcement in its efforts to combat crime. At the same time, we wanted to find ways to assure continued U.S. technology leadership, promote secure electronic commerce, and protect privacy concerns. We believed then and now that the best way to make progress on this issue is through a constructive, cooperative dialogue, rather than by legislative solutions. Through dialogue lasting more than a year, there has been increased understanding among the parties and we have made progress.

On December 31, we published regulations implementing the Vice President's policy announcement. These regulations will not end the debate over encryption controls, but we believe the regulation addresses some private sector concerns by opening large markets and further streamlining exports.

The Update permits the export of 128-bit encryption products and higher (with or without key recovery) to several important industry sectors. Now, banks, financial institutions, health facilities, and on-line merchants can secure their sensitive financial, medical, and on-line transactions in digital form. This update also allows U.S. companies to export 128-bit or greater encryption products, including technology to subsidiaries around the world, to protect its proprietary information and to develop new products. Further, this update allows the export of 128-bit or greater "recovery capable" or "recoverable" encryption products under an encryption licensing arrangement. Such products include those that are readily available in the marketplace such as general purpose routers, firewalls, and virtual private networks. These recoverable products are usually managed by a network or corporate security administrator without any involvement by a third party. Since the Update announcement, Industry has been taking advantage of this new liberalization and the streamlined process awarded to such products.

Many of the updates permit the export of encryption to these end-users under a license exception. That is, after the product receives a technical review, it can be exported by manufacturers, resellers and distributors without the need for a license or other additional review. These license exceptions currently apply to a list of countries or a set of end users. We also have a general policy of approval for exports to those sectors through encryption licensing arrangements (ELA), a kind of bulk license, to allow unlimited shipments of strong encryption to the sectors worldwide.

We also further streamlined exports of key recovery products by no longer requiring a review of foreign key recovery agents and no longer requiring companies to submit business plans.

We recognize that the development of our policy is an evolutionary process, and we intend to continue our dialogue with industry. Our policy will continue to adapt to technology and market changes. We will review our policy again this year with a view toward making further changes. An important component of our review is input from industry, which we are receiving through our continuing dialogue.

This past year, we also made progress on developing a common international approach to encryption controls through the Wassenaar Arrangement. Established in 1996 as the successor to COCOM, it is a multilateral export control arrangement among 33 countries whose purpose is to prevent destabilizing accumulations of arms and industrial equipment with military uses in countries or regions of concern. Wassenaar provides the basis for many of our export controls.

In December, through the hard work of Ambassador David Aaron, the President's special envoy on encryption, the Wassenaar Arrangement members agreed on several changes relating to encryption controls. These changes go a long way toward increasing international security and public safety by providing countries with a stronger regulatory framework for managing the spread of robust encryption. Specific changes to multilateral encryption controls include removing multilateral controls on all encryption products at or below 56 bit and certain consumer items regardless of key length, such as entertainment TV systems, DVD products, and on cordless telephone systems designed for home or office use.

Most importantly, the Wassenaar members agreed to remove encryption software from Wassenaar's General Software Note and replace it with a new cryptography note. Drafted in 1991, when banks, government and militaries were the primary users of encryption, the General Software Note allowed countries to export mass market encryption software without restriction. The GSN was created to release general purpose software used on personal computers, but it inadvertently also permitted countries to release encryption. It was essential to modernize the GSN and close the loophole that permitted the uncontrolled export of encryption with unlimited key length. Under the new cryptography note, mass market hardware has been added and a 64-bit key length or below has been set as an appropriate threshold. This will lead governments to review the dissemination of 64-bit and above encryption.

I want to be clear that this does not mean encryption products of more than 64 bits cannot be exported. Our own policy permits that, as does the policy of most other Wassenaar members. It does mean, however, that such exports now can be reviewed by governments consistent with their national export control procedures.

Export control policies without a multilateral approach have little chance of success. Agreement among the Wassenaar members on the treatment of mass market encryption products is a strong indication that other countries share our public safety and national security concerns. Contrary to what many people thought two years ago, we have found that most major encryption producing countries are interested in developing a common approach to encryption controls.

THE PROTECT ACT

With respect to S. 789, the Administration opposes this legislation for a number of reasons. Overall the bill does not promote the balance that this Administration has worked so hard to achieve over the past several years. Let me now discuss some of the more problematic sections.

Under section 505, the removal of export controls on publicly or generally available encryption is in effect left to an advisory board composed of private sector and government representatives, with the concurrences of the Secretary. We believe such a board would be unworkable. Although availability is one of the factors we use to decide whether an encryption product may be exported, it is not the only factor and should not be elevated above the others. We need to be able to take all factors, including national security and public safety, into account when making export control decisions. Disallowing or downgrading important considerations will only serve to weaken our export control system. The broad definitions used in the bill would give the Board wide latitude in making its findings on what is available. This could place the Secretary in the position of having to routinely object to the removal of export controls when important national security and law enforcement interests are at stake. The bill makes this decision subject to judicial review. The Administration does not think it is wise public policy for the courts to adjudicate Executive Branch decisions on these matters.

Section 501 removes the Department of Justice from the encryption export license consultation process. Since law enforcement interests are an important consideration in regard to encryption, we cannot support this provision.

We support the provisions in the bill that require a technical review for eligibility to export encryption under a license exception. In fact, this is consistent with current regulations. What we cannot support, however, is the portion of section 504 that would provide automatic eligibility after 15 days if the exporter has not received a decision from the government. In all cases, a very careful technical review is completed in order to determine that a product is technically eligible for a particular license exception. Although we try to perform these reviews as quickly as possible, a 15-day automatic approval will severely limit our ability to do a careful review.

Section 504 also proposes control parameters and export liberalizations beyond what the Administration can entertain and which would be contrary to our international export control obligations. For example, Wassenaar agreed to decontrol encryption products up to 56-bits whereas this bill would decontrol encryption products using a key length at 64-bits or less. Section 504 also expands the set of products, end users, and countries eligible to receive encryption under a license exception beyond what we believe is prudent.

Another troubling part of this bill is section 102, which would permit a U.S. person located anywhere in the world to develop, manufacture, sell or use any type of encryption. If this provision were construed to permit U.S. citizens to develop, manufacture and sell encryption products overseas, even with the use of non-public controlled technology that they had acquired in the United States, it would, in effect, prevent the government from requiring a license for U.S. persons to develop and manufacture encryption abroad. As a result, U.S. companies would likely move all development and manufacture of encryption out of the United States in order to take advantage of this loophole. This is not in our country's economic or national security interest.

Section 103 contains a provision that would prohibit the U.S. Government from conditioning any approval on the fact that a product is recoverable. A fundamental feature of our encryption policy is that we provide incentives for companies to develop products that provide strong security and also meet the needs of national security and law enforcement. The bill would eliminate this laudable feature of our policy that industry wanted us to include in last year's update. In addition, this provision of the bill is inconsistent with section 504 which allows license exception treatment for recoverable products.

Section 506 would eliminate any export controls on products using the forthcoming Advanced Encryption Standard (AES). We oppose the removal of export controls on encryption products simply because they implement a government standard. Products incorporating the AES should be exportable to the same extent as any other product incorporating encryption of similar strength. Under our current policy, AES-based products could be exported to banks, large corporations, on-line merchants without restriction and to many other safe endusers depending on the nature of the product. We do not think it is wise to link development of the AES to export controls. Such a linkage might bring undue pressure on NIST to complete the AES process faster than planned, and may therefore not allow prudent study of the security features of the candidate algorithms before selection.

With respect to the provisions of the bill that do not relate to export controls, we have a number of questions and concerns.

One such provision in Section 202 requires that encryption products used by the Government must interoperate with other commercial encryption products. The extent to which interoperability is required is unclear in the bill, but we believe the practical result of this requirement is that the Government could not use encryption because no single encryption product interoperates with all other products. It also appears that this provision could prohibit the use of encryption developed by the government for its own internal use in "closed" systems that are purposefully designed not to interoperate with other systems.

Section 202 also appears to prevent mandatory use of recoverable encryption when communicating with U.S. Federal, state and local governments. This would appear to preclude an agency from requiring key recovery or recoverable products for business purposes. We believe the effect of this provision may be much broader than simply preventing government from using recoverable encryption when dealing with the public. The practical effect would be that Government sites would have to be capable of supporting secure communications using all encryption methodologies on the market. This is absurd.

We are concerned that section 302 of the bill may preclude NIST's work with voluntary standards organizations because it prohibits the Secretary of Commerce from carrying out any policy that establishes an encryption standard for use by businesses or other entities other than for computer systems operated by the United States Government. The Secretary of Commerce is prohibited from establishing

standards for business; however, when invited by standards organizations to do so, NIST does, as a matter of policy, work together with those organizations. Cooperation between NIST and standards organizations is important for both NIST and industry, and it is consistent with government policy to use voluntary standards and to purchase commercial off-the-shelf products. If the government cannot have input to the standards process, we may end up with less secure products available for government agencies. We want to encourage, to the extent possible, the development of voluntary standards that meet the needs of the government. This reduces costs for both government and industry.

In regard to section 401 dealing with the "Information Technology Laboratory," we have two concerns. First, we do not think it is appropriate for NIST to undertake research and development of new technologies to facilitate lawful access to communications and electronic information. This activity is more appropriately done by the FBI. Second, we are concerned that the bill will provide NIST with new tasks but no new funding to carry out this work. We have similar concerns with section 402. The advisory board, whose correct statutory name is "Computer System Security and Privacy Advisory Board," is made up of 13 volunteers. Again, any additional tasks assigned to this board would require necessary funding.

The Administration does not seek encryption export control legislation, nor do we believe such legislation is needed. The current regulatory structure provides for balanced oversight of export controls and the flexibility needed to adjust to our economic, foreign policy and national security interests to advances in technology. This is the best approach to an encryption policy that promotes secure electronic commerce, maintains U.S. lead in information technology, protects privacy, and protects public safety and national security interests.

As you know, public debate over encryption policy has been lively and often acrimonious. Some of those on both sides of the debate are not interested in searching for a middle ground that can meet all of our needs. Our dialogue with industry has gone a long way toward bridging that gap and finding common ground. We will continue this policy of cooperative exchange, which is clearly the best way to pursue our policy objectives of balancing public safety, national security, and the competitive interests of U.S. companies.

Senator BURNS. Thank you, Mr. Secretary. I want to also thank you for the dialog we have had. We are not new to this debate. We have been going through it. But we have learned, I think, from each other. It is enlightening to know how the evolution of the mind set changes as technology moves forward.

We are pleased to welcome Jim Robinson, Assistant Attorney General for the Criminal Division. Thank you for coming this morning.

STATEMENT OF HON. JAMES K. ROBINSON, ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, U.S. DEPARTMENT OF JUSTICE

Mr. ROBINSON. Mr. Chairman, members of the committee: I appreciate the opportunity to appear to—

Senator BURNS. Do you want to pull the microphone a little closer to you.

Mr. ROBINSON. I will, Senator. Thank you.

I appreciate the opportunity to present the views of the Justice Department on the issue of encryption and export controls. As you would expect, the Justice Department is particularly interested in the important public safety interests implicated in the encryption debate. I would like to emphasize some of the key points outlined in my written statement submitted to the committee and to place those thoughts in a more personal context.

When I took office as the Assistant Attorney General for the Criminal Division about a year ago this month, I quickly learned how important the encryption debate is to law enforcement. I served as the U.S. Attorney for the eastern district of Michigan

from 1977 to 1980. From a technological point of view, the world was a very different place in those days, both for our society in general and certainly for law enforcement.

Technological advances have made important new tools available to law enforcement for the successful investigation and prosecution of criminal activity. These tools have enhanced law enforcement's ability to protect public safety and to achieve just results. The use of DNA evidence is a prime example. DNA evidence can not only provide strong evidence of guilt, it can be powerful evidence of innocence.

Technology has also enhanced law enforcement's capacity for early detection and prevention of criminal acts. But technological progress has also had its costs. The potential dark side of this progress is that well-financed criminal elements are also using new technology to commit crimes, avoid detection, and to cover their tracks. Traditional highly-effective law enforcement techniques are threatened by these developments.

The issue of encryption starkly presents both aspects of technological progress. Encryption supports public safety and law enforcement by protecting sensitive and personal information from unauthorized access. Encryption is therefore, as many have said here this morning, an absolutely essential tool for preventing crime in the information age.

The Department is, however, deeply concerned about the other side of encryption, the threat to public safety posed by the widespread use of nonrecoverable encryption by criminals. Thus the Justice Department supports the spread of strong recoverable encryption both to protect the privacy and safety of American citizens and the security of our information infrastructure.

Assessing the benefits versus the risks of encryption for law enforcement in today's world is complex enough, but the issue is made even more complex and problematic by the expanding use of global information networks like the Internet. Technological advances in electronic commerce and communication, as we all know, have led to the explosive growth of the Internet. This development has made the use of robust encryption essential for protecting the privacy and security of communications and stored electronic data.

This new technology, however, has also made it possible for international criminals and terrorists to target America in an unprecedented number of ways, such as fraud over the Internet, computer hacking, economic and governmental espionage, and cyberterrorism. We are also seeing a dramatic growth of international crime with grave potential consequences for the Nation.

Law enforcement must be concerned not only with the use of encryption by domestic criminals, but increasingly we must be concerned by the ability of foreign criminals and terrorists to target America and use robust encryption to hide their criminal activity. Law enforcement agencies in the United States and abroad have already begun to see cases where encryption has been used in an attempt to conceal criminal activity. The number and complexity of these cases will certainly increase as increasingly powerful encryption proliferates.

As this committee considers the issue of encryption, we trust that it will consider also, as we know it will, the very real cost to public

safety that the use of nonrecoverable encryption by terrorists, drug dealers, and other criminals will pose. Faced with the use of such encryption, agents frequently and increasingly will be unable to make effective use of search warrants, wiretap orders, and other legal processes authorized by Congress and sanctioned by the courts. Law enforcement will find it increasingly difficult to obtain important evidence of criminal activities. Critical evidence to support successful prosecution may simply be unavailable. In short, this will mean that fewer crimes will be prevented and fewer criminals will be caught, prosecuted, and taken off the streets.

Despite these challenges to effective law enforcement, we cannot and must not ignore the significant benefits of encryption. That is why the Department supports a carefully balanced approach to export controls, an approach that seeks to encourage the favorable uses of encryption while minimizing its negative effects on public safety and national security. The Department believes that the rapid elimination of export controls as proposed in the PROTECT Act would upset this delicate balance. It is likely that the passage of this act would cause in the near term the easy acquisition of robust nonrecoverable encryption products, not only by people we want to have them, but by terrorist organizations and international criminals on a global scale. This development will substantially frustrate the ability of law enforcement to combat international criminal activity.

Instead of encryption decontrol, we believe that a continuing dialogue offers the best hope of developing workable solutions to the encryption dilemma. Law enforcement has been engaging industry leaders in a continuing and cooperative dialogue in an attempt to work toward voluntary solutions that accommodate the needs of privacy, electronic commerce, national security, and public safety. We will continue to work hard to make sure that these productive discussions will continue to bear fruit.

We are realists. We understand that no matter what solutions industry develops and no matter what policy is adopted by the Administration and by Congress, some criminals will obtain and use robust nonrecoverable encryption that will deny law enforcement the ability to obtain useable evidence. We cannot afford to stand still while technology passes us by. Therefore, in addition to an intensive dialogue with industry and continuing to work with the international community on this important topic, law enforcement must continue developing its own technical expertise to deal effectively with encrypted evidence of criminal activity.

The Department has begun initiatives such as the funding of a centralized technical resource within the FBI which will support Federal, State and local law enforcement personnel in developing a broad range of expertise, technologies, and tools to respond directly to the threat to public safety posed by the use of encryption by criminals and terrorists.

In conclusion, we believe that an approach that balances the need for secure private communications and data storage with the equally important need to protect the safety of the public against threats from terrorists and criminals is the best policy.

We appreciate your willingness to consider these important public safety concerns and we look forward to working with you on this important issue. Thank you very much.

[The prepared statement of Mr. Robinson follows:]

PREPARED STATEMENT OF JAMES K. ROBINSON, ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, U.S. DEPARTMENT OF JUSTICE

Mr. Chairman, thank you for the opportunity to testify about the Department of Justice's views on encryption, and particularly the proposed Promote Reliable On-Line Transactions to Encourage Commerce and Trade (PROTECT) Act, introduced by you as S. 798. As you are aware, encryption, and specifically export controls on encryption, presents complex and difficult issues that we are attempting to address with our colleagues throughout the Administration. In my testimony, I will first outline the basic perspective and recent initiatives of the Department of Justice on encryption issues, and will then discuss some specific concerns with the PROTECT Act.

ENCRYPTION, THE LAW ENFORCEMENT PERSPECTIVE

The Department of Justice supports the spread of strong, recoverable encryption. Law enforcement's responsibilities and concerns include protecting privacy and commerce over our nation's communications networks. For example, we prosecute under existing laws those who violate the privacy of others by illegal eavesdropping, computer hacking or theft of confidential information. Over the last few years, the Department has continually pressed for laws protecting confidential information and the privacy of citizens. Furthermore, we help protect commerce by enforcing the laws, including those that protect intellectual property rights, and that combat computer and communications fraud. (In particular, we help to protect the confidentiality of business data through enforcement of the recently enacted Economic Espionage Act.) Our support for robust encryption is a natural outgrowth of our commitment to protecting privacy for personal and commercial interests. As the head of the Criminal Division of the Department of Justice, I hold these values dear.

But the Department of Justice protects more than just privacy. We also protect public safety and national security against the threats posed by terrorists, organized crime, foreign intelligence agents, and others. Moreover, we have the responsibility for preventing, investigating, and prosecuting serious criminal and terrorist acts when they are directed against the United States. We are gravely concerned that the proliferation and use of non-recoverable encryption by criminal elements would seriously undermine these duties to protect the American people. Therefore, we favor the spread of strong encryption products that permit timely and legal law enforcement access to plaintext.

The most easily understood example is electronic surveillance. Court-authorized wiretaps have proven to be one of the most successful law enforcement tools in preventing and prosecuting serious crimes, including drug trafficking and terrorism. We have used legal wiretaps to bring down entire narcotics trafficking organizations, to rescue young children kidnaped and held hostage, and to assist in a variety of matters affecting our public safety and national security. In addition, as society becomes more proficient in its use of computers, evidence of crimes is increasingly found in stored computer data, which can be searched and seized pursuant to court-authorized warrants. But if non-recoverable encryption proliferates, these critical law enforcement tools would be nullified. Thus, for example, even if the government satisfies the rigorous legal and procedural requirements for obtaining a wiretap order, the wiretap would be worthless if the intercepted communications of the targeted criminals amount to an unintelligible jumble of noises or symbols. Or we might legally seize the computer of a terrorist and be unable to read the data identifying his or her targets, plans and co-conspirators. The potential harm to public safety, law enforcement, and to the nation's domestic security could be devastating.

I want to emphasize that this concern is not theoretical, nor is it exaggerated. Although use of encryption is far from universal, we have already begun to encounter its harmful effects. For example, in an investigation of a multinational child pornography ring, investigators discovered sophisticated encryption used to conceal thousands of images of child pornography that were exchanged among members. Similarly, in several major computer hacker cases, the subjects have encrypted computer files, thereby concealing evidence of serious crimes. In one such case, the government was unable to determine the full scope of the hacker's activity because of the use of encryption. Finally, criminal use of encryption is becoming increasingly international—the United Kingdom recently reported that in 1996 it seized encrypted

files from a Northern Irish terrorist group concerning terrorist targets such as police officers and politicians. In that case, law enforcement was able to read the data, but only after considerable effort.

The lessons learned from these investigations are clear: criminals are beginning to learn that encryption is a powerful tool for keeping their crimes from coming to light. Moreover, as encryption proliferates and becomes an ordinary component of mass market items, and as the strength of encryption products increases, the threat to public safety will increase proportionately.

Given both the benefits presented and risks posed by encryption, the Department believes that encouraging the use of recoverable encryption products—which protect business and personal data as well as public safety—is an important part of the Administration's balanced encryption policy. Recoverable products also fulfill business needs. Information technology companies have told us that their customers recognize the need to ensure recoverability of their data when using strong encryption; otherwise, they risk losing access to their data forever. For example, a company might find that one of its employees lost his encryption key, thus accidentally depriving the business of important and time-sensitive business data. We should point out that loss of an encryption key is not theoretical. One company told us that employees commonly lose or forget their passwords, which must then be restored by system administrators. The same capability must exist for encryption systems. Similarly, a business may find that a disgruntled employee has encrypted confidential information and then absconded with the key. In these cases, a plaintext recovery system promotes important private sector interests. Indeed, as the Government implements encryption in our own information technology systems, it also has a business need for plaintext recovery to assure that data and information that we are statutorily required to maintain are in fact available at all times. For these reasons, as well as to protect public safety, the Department has been affirmatively encouraging the voluntary development of "plaintext" recovery products, recognizing that only their ubiquitous use will provide both protection for data and protection of public safety. We also want to underscore that in most recoverable systems, businesses will manage their own keys.

Because we remain concerned with the impact of encryption on the ability of law enforcement at all levels of government to protect the public safety, the Department and the FBI are engaged in continuing discussions with industry in a number of different fora. These ongoing, productive discussions seek to find creative solutions, in addition to key recovery, to the dual needs for strong encryption to protect privacy and plaintext recovery to protect public safety and business interests. While we still have work to do, these dialogues have been useful because we have discovered areas of agreement and consensus, and have found promising areas for seeking compromise solutions to these difficult issues. While we do not think that there is one magic technology or solution to all the needs of industry, private citizens, and law enforcement, we believe that by working with those in industry who create and market encryption products, we can benefit from the accumulated expertise of industry to gain a better understanding of technology trends and develop advanced tools that balance privacy and security.

Furthermore, we believe that a constructive dialogue on these issues is the best way to make progress, rather than export control legislation. Although export controls on encryption products have been in place for years and exist primarily to protect national security and foreign policy interests, they are in no sense inflexible, and have been updated in recent years in a continuing effort to balance the needs of privacy, electronic commerce, public safety, and national security. Indeed, largely as a result of the dialogue the Administration has had with industry, significant progress has been made on export controls. Recent updates were announced by Vice President Gore on September 16, 1998, and implemented in an interim rule, which was issued on December 31, 1998. The Department of Justice supports these updates to export controls, which permit the export of products that have a bit length of 56-bits or less, and also permit the easy export of unlimited-strength encryption to certain industry sectors, including medical facilities and banks, financial institutions, and insurance companies in most jurisdictions. These changes allow these sectors, which possess large amounts of highly sensitive and personal information, to use products that will protect the privacy of their clients. The Administration also expanded its policy to permit recoverable exports, such as encryption systems managed by network administrators, to foreign commercial firms. We learned about these systems through our dialogue with industry. According to industry, such systems are demanded by the market today and are in use. They are also largely consistent with the needs of law enforcement.

The Department, in conjunction with the rest of the Administration, intends to continue our dialogue with industry, and will evaluate the export control process on

an ongoing basis in order to ensure that the balance of interests remains fair to all concerned. We agree that there are a wide range of national interests that must be supported, including U.S. industry competitiveness. Hence, we are committed to continued review and dialogue with industry.

At the same time, we must recognize that market forces will only take us so far. To the extent that criminal activity, such as terrorism or child pornography, occurs outside the business environment, criminals would rather lose data than have it seized by law enforcement. Thus, more must be done. Therefore, the Department of Justice is also trying to address the threat to public safety from the widespread use of encryption by enhancing the ability of the Federal Bureau of Investigation and other law enforcement entities to obtain the plaintext of encrypted communications. Among the initiatives is the funding of a centralized technical resource within the FBI. This resource, when fully established, will support federal, state, and local law enforcement in developing a broad range of expertise, technologies, tools, and techniques to respond directly to the threat to public safety posed by the widespread use of encryption by criminals and terrorists. It will also allow law enforcement to stay abreast of rapid changes in technology. Finally, it will enhance the ability of law enforcement to fully execute the wiretap orders, search warrants, and other lawful process issued by courts to obtain evidence in criminal investigations when encryption is encountered. However, we must recognize that these efforts—while critical—do not (like market forces) alone provide an adequate solution to the encryption problem, as the widespread use of non-recoverable encryption by criminals would quickly overwhelm any possible law enforcement technical response.

THE PROTECT ACT

In light of the above, the proposed Promote Reliable On-Line Transactions to Encourage Commerce and Trade Act raises several concerns from the perspective of the Department of Justice. First, the Act may impede the voluntary development of products that could assist law enforcement in obtaining access to plaintext. The Administration believes that the development of such products is important for a safe society. For example, the Act might preclude the United States government from utilizing useful and appropriate incentives to develop or use key recovery techniques, such as purchasing key recovery products for its own use and supporting pilot projects that demonstrate the viability of key recovery.

Second, the Act also could impair the government's ability to engage in secure electronic commerce. We are concerned that the breadth of the language in subsection 202(c) may limit the ability of an agency to require a certain type of authentication mechanism for transactions between the public and the government. (For example, in the context of an electronic filing of a regulatory report, a tax return, or an application for benefits, authentication of the filer's identity is critical, including for any subsequent enforcement action.) This concern is raised because the definition of "encryption" includes the use of mathematical formulas to preserve not only confidentiality, but also integrity or authenticity.

Third, the PROTECT Act places responsibility for developing techniques for obtaining lawful access to the plaintext of communications and data in the National Institute for Standards and Technology (NIST). As I noted above, the Department of Justice has already begun to create a centralized technical resource within the FBI to develop a broad range of expertise, technologies, tools, and techniques to respond to the use of encryption by criminals and terrorists. In my view, the responsibility for developing such tools and techniques should in this case lie with law enforcement, because it is law enforcement that has the operational expertise to understand the requirements for such tools and techniques to be effective. Moreover, it is law enforcement that will actually have to put the techniques into practice. Instead of conferring this new responsibility on NIST, I would request that Congress continue to support our efforts to develop technical expertise within the law enforcement community.

Fourth, we share the deep concern of the National Security Agency that the proposed PROTECT Act would harm national security and public safety interests through the liberalization of export controls far beyond our current policy. Among other decontrols, the proposed Act provides that a product is to be exportable if a product of equivalent strength or key length will be available outside the United States in the next 12 months—even if the product of supposedly equivalent strength is intended for different uses, is not user-friendly or widely used, is not cost-competitive, or does not present the same threats to national security. We are concerned that this considerable decontrol of robust encryption will cause in the near term the easy acquisition of robust encryption products by terrorist organizations and inter-

national criminals and frustrate the ability of law enforcement to combat these problems internationally. Moreover, the structure and functions of the proposed Encryption Export Advisory Board raise concerns under separation of powers principles and the Appointments Clause.

It is also important to consider that our allies concur that unrestricted export of encryption poses a significant risk to national security, especially to regions of concern. As recently as December 1998, the thirty-three members of the Wassenaar Arrangement reaffirmed the importance of export controls on encryption for national security and public safety purposes and adopted agreements to enable governments to review exports of hardware and software with a 56-bit key length and above and mass-market products above 64 bits, consistent with national export control procedures. Thus, the elimination of U.S. export controls, as provided by the proposed Act, would severely hamper the international community's efforts to combat such international public safety concerns as terrorism, narcotics trafficking, and organized crime.

In light of these factors, we believe that the Administration's more cautious balanced approach is the best way to protect our commercial interests, including our interest in ensuring the success of U.S. industry and electronic commerce, while simultaneously protecting law enforcement and national security interests. We believe that legislation that eliminates or substantially reduces export controls on encryption could upset that delicate balance and is unwise.

The recent decision of the United States Court of Appeals for the Ninth Circuit in *Daniel Bernstein* v. *United States Department of Justice and United States Department of Commerce* has not changed our view that legislation eliminating or substantially reducing export controls is contrary to our national interests. The Department of Commerce and the Department of Justice are currently reviewing the Ninth Circuit's decision in *Daniel Bernstein* v. *United States Department of Justice and United States Department of Commerce,* and we are considering possible avenues for further review, including seeking a rehearing of the appeal *en banc* in the Ninth Circuit. In the interim, the regulations controlling the export of encryption products remain in full effect, even as to Professor Bernstein's own software.

In sum, we as government leaders should embark upon the course of action that best preserves the balance long ago set by the Framers of the Constitution, preserving both individual privacy and society's interest in effective law enforcement. We should promote encryption products which contain robust cryptography but that also provide for timely and legal law enforcement access to encrypted evidence of criminal activity. We should also find ways to support secure electronic commerce while minimizing risk to national security and public safety. This is the Administration's approach. We look forward to working with this Committee as it enters the markup phase of this bill.

Senator BURNS. Thank you very much. We will get into some questions this morning in a few moments.

We welcome this morning Barbara McNamara, Deputy Director, National Security Agency. Thank you for coming this morning.

STATEMENT OF BARBARA A. MCNAMARA, DEPUTY DIRECTOR, NATIONAL SECURITY AGENCY

Ms. MCNAMARA. Thank you, Mr. Chairman, members.

Senator BURNS. Pull up that microphone a little. You have such a sweet, soft voice.

Ms. MCNAMARA. Thank you, Mr. Chairman. There are other people in this room who would probably take issue with that comment, but I am pleased to hear it.

Senator BURNS. They are not the chairman.

Ms. MCNAMARA. But thank you very much, and it is a pleasure to be here today to talk about this particular bill and its impact on national security from NSA's standpoint.

NSA plays a critical role in our national security. We intercept and analyze the communications signals of foreign adversaries to produce critically unique and actionable intelligence reports for our national leaders and military commanders. Very often time is of

the essence. Intelligence is perishable. It is worthless if we cannot get it to the decision-maker in time to make a difference.

Signals intelligence proved its worth in World War II when the United States broke the Japanese naval code and learned of their plans to invade Midway Island. This significantly aided the U.S. defeat of the Japanese fleet and helped shorten the war. Today NSA is providing that same kind of intelligence support to our troops in the former Yugoslavia and other locations around the world wherever U.S. military forces are deployed.

Demands on NSA for timely intelligence have only grown since the breakup of the Soviet Union and have expanded into national security areas of terrorism, weapons proliferation, and narcotics trafficking. Currently many of the world's communications are unencrypted. If not controlled, encryption will spread and be widely used by foreign adversaries that have traditionally relied upon unencrypted communications. As a result, much of the crucial information we are able to provide today could quickly become unavailable to U.S. decision-makers.

As you review the PROTECT Act, it is very important that you understand the significant effect certain provisions of this bill will have on national security. In particular, NSA is concerned about the establishment of an Encryption Export Advisory Board heavily weighted to private sector representation. This effectively cedes control over U.S. export policy to the private sector.

Furthermore, the board is to base its recommendation for export on the foreign availability or public availability of comparable products. In the interests of national security, encryption export policy should not and cannot be based solely on foreign availability.

The PROTECT Act calls for the export of a product greater than 64 bits if it will generally be widely available from a foreign supplier within the next 12 months. Any policy based on the foreign or public availability of a comparable product, especially a year in advance of its actual appearance in the marketplace, will force administration policy to be driven by unfounded market trends without consideration of national security or foreign policy interests.

Foreign products are often not as widely used as reported, as secure as advertised, or as easy to use for lack of an infrastructure as represented. In many cases, a foreign encryption product is subject to the export controls of the country in which it is manufactured. In the case of the other 32 Wassenaar nations, an encryption product is held to the same or similar standards as U.S. products.

In addition, there are other important concerns that must be taken into consideration when deciding if a product should be exported, such as to whom the product is exported and for what purpose. In that regard, the PROTECT Act also eliminates the end user reporting that is so valuable to national security.

The PROTECT Act permits strong encryption products to be approved under a license exception for export to so-called "trustworthy entities and regions" without prior government knowledge of intended end users. These include any foreign partners of U.S. companies, other governments, and almost any foreign commercial firm in any country. Some end users could in fact be targets of national security interests, such as narcotics traffickers.

The PROTECT Act also automatically decontrols the export of strong encryption in the form of systems using the Advanced Encryption Standard to any destination upon adoption of AES, but at least by January 1, 2002. While current U.S. policy has opened up many sectors in many nations, it has done this in a thoughtful manner that miniminizes the risks to important national security interests. The PROTECT Act upsets this delicate balance by widely expanding exports without due consideration to national security.

Finally, the PROTECT Act's 15-day technical review period is too rigid to permit a meaningful technical review. The government needs the opportunity to review a proposed export to assure it is compatible with U.S. national security interests and requires the ability to deny an export application if national security concerns are not adequately addressed.

The ability to know what is being considered for export is a key part of U.S. export control policy. In some cases today, this process takes longer than 15 days because insufficient information is provided as part of the initial application.

Let me make it clear. We want U.S. companies to effectively compete in world markets. In fact, it is something that we strongly support as long as it is consistent with national security needs.

In summary, the PROTECT Act will harm national security. It will make NSA's job of providing critical actionable intelligence to our leaders and military commanders difficult, if not impossible, thus putting our Nation's security at considerable risk. The United States cannot have an effective decision-making process or a strong fighting force or a responsive law enforcement community or a strong counterterrorism capability unless the information required to support them is available in time to make that difference.

Thank you, gentlemen.

[The prepared statement of Ms. McNamara follows:]

PREPARED STATEMENT OF BARBARA A. MCNAMARA, DEPUTY DIRECTOR, NATIONAL SECURITY AGENCY

Mr. Chairman, thank you for giving me the opportunity today to discuss the important issue of encryption. I will be discussing the national security needs for export controls on encryption and why we oppose legislation that would effectively lift those controls. I will then address specific concerns NSA has with provisions of the PROTECT Act. However, I should like to begin by briefly introducing the National Security Agency (NSA) and its mission.

The National Security Agency was founded in 1952 by President Truman. As a separately organized agency within the Department of Defense, NSA provides signals intelligence to a variety of users in the Federal Government and secures information systems for the Department of Defense and other U.S. Government agencies. NSA was designated a Combat Support Agency in 1988 by the Secretary of Defense in response to the Goldwater-Nichols Department of Defense Reorganization Act.

The ability to understand the secret communications of our foreign adversaries while protecting our own communications—a capability in which the United States leads the world—gives our nation a unique advantage. The key to this accomplishment is cryptology, the fundamental mission and core competency of NSA. Cryptology is the study of making and deciphering codes, ciphers, and other forms of secret communications. NSA is charged with two complementary tasks in cryptology: first, exploiting foreign communications signals and second, protecting the information critical to U.S. national security. By "exploitation," I am referring to signals intelligence, or the process of deriving important intelligence information from foreign communications signals; by "protection" I am referring to providing security for information systems. Maintaining this global advantage for the United States requires preservation of a healthy cryptologic capability in the face of unparalleled technical challenges.

It is the signals intelligence (SIGINT) role that I want to address today. Our principal responsibility is to ensure a strong national security environment by providing timely information that is essential to critical military and policy decision making. NSA intercepts and analyzes the communications signals of our foreign adversaries, many of which are guarded by codes and other complex electronic countermeasures. From these signals, we produce vital intelligence reports for national decision makers and military commanders. Very often, time is of the essence. Intelligence is perishable; it is worthless if we can not provide it in time to make a difference in rendering vital decisions.

For example, SIGINT proved its worth in World War II when the United States broke the Japanese naval code and learned of their plans to invade Midway Island. This intelligence significantly aided the U.S. defeat of the Japanese fleet. Subsequent use of SIGINT helped shorten the war. NSA continues today to provide vital intelligence to the warfighter and the policy maker in time to make a difference for our nation's security. Demands on us in this arena have only gown since the breakup of the Soviet Union and have expanded to address other national security threats such as terrorism, weapons proliferation, and narcotic trafficking, to name a few.

Because of these growing serious threats to our national security, care must be taken to protect our nation's intelligence equities. Passage of legislation that decontrols the export of strong encryption will significantly harm NSA's ability to carry out our mission and will ultimately result in the loss of essential intelligence reporting. This will greatly complicate our exploitation of foreign targets and the timely delivery of intelligence to decision makers because it will take too long to decrypt a message—if indeed we can decrypt it at all.

Today, many of the worst's communications are unencrypted. Historically, encryption has been used primarily by governments and the military. It was employed for confidentiality in hardware-based systems and was often cumbersome to use. As encryption moves to software-based implementations and the infrastructure develops to provide a host of encryption-related security services, encryption will spread and be widely used by other foreign adversaries that have traditionally relied upon unencrypted communications. The decontrol of encryption exports would accelerate the use of encryption by many of these adversaries and as a result, much of the crucial information we are able to gather today could quickly become unavailable to us. National security must have an opportunity to conduct a meaningful review of encryption products prior to their export. In the past, this review process has provide us with valuable insight into what is being exported, to whom, and for what purpose. Without this review and the ability to deny an export application, it will be impossible to control exports of encryption to individuals and organizations that threaten the United States. For instance, decontrol will undermine international efforts to prevent terrorist attacks, and catch terrorists, drug traffickers, and proliferators of weapons of mass destruction.

Please do not confuse the needs of national security with the needs of law enforcement. The two sets of interests and methods vary considerably and must be addressed separately. The law enforcement community is primarily concerned about the use of non-recoverable encryption by persons engaged in illegal activity. At NSA, we are primarily focused on preserving export controls on encryption to protect national security.

While our mission is to provide intelligence to help protect the country's security, we also recognize that there must be a balanced approach to the encryption issue. The interests of industry and privacy groups, as well as of the Government, must be taken into account. Encryption is a technology that will allow our citizens to fully participate in the 21st Century world of electronic commerce. It will enhance the economic competitiveness of U.S industry. It will combat unauthorized access to private information and it will deny adversaries from gaining access to U.S. information wherever it may be in the world.

To promote this balanced approach, we are engaged in an ongoing and productive dialogue with industry. The recent Administration update to the export control regulations addresses many industry concerns and has significantly advanced the ability of U.S. vendors to participate in overseas markets. Of equal significance, the Wassenaar nations, representing most major producers and users of encryption, agreed unanimously in December 1998 to control strong hardware and software encryption products. The Wassenaar Agreement clearly shows that other nations agree that a balanced approach is needed on encryption policy and export controls so that commercial and national security interests are addressed. Both are positive developments because they open new opportunities for U.S. industry while still protecting national security. These are examples of the kinds of advances possible under the current regulatory structure, which provides greater flexibility than a statutory structure to adjust export controls as circumstances warrant in order to

meet the needs of Government and industry. We want U.S. companies to effectively compete in world markets. In fact, it is something we strongly support as long as it is done consistently with national security needs NSA supports the recent updates to the Administration's policy. The export provisions were carefully designed to open up large commercial markers while tying to minimize potential risk to national security. We believe significant progress was made.

As you review the PROTECT Act, it is very important that you understand the significant effect certain provisions of this bill will have on national security. In particular, NSA is concerned about the establishment of an Encryption Export Advisory Board, heavily weighted to private sector representation. This effectively cedes control over U.S. encryption export policy to the private sector. Furthermore, the Board is to base its recommendation for export on the foreign availability or public availability of comparable products. In the interests of national security, encryption export policy should not be based solely on foreign availability or public availability. The PROTECT Act calls for the export of a product greater than 64-bits if it will be generally or widely available from a foreign supplier within the next twelve months. Any policy based on the foreign or public availability of a comparable product, especially a year in advance of its actual appearance in the marketplace, will force Administration policy to be driven by unfounded market trends without consideration of national security or foreign policy interests.

Foreign products are often not as widely used as reported, as secure as advertised, or as easy use (for lack of an infrastructure) as represented. In many cases, a foreign encryption product is subject to the export controls of the country in which it is manufactured. In the case of the other 32 Wassenaar nations, an encryption product is held to the same, or similar, standards as U.S. products. In addition, there are other important concerns that must be taken into consideration when deciding if a product should be exported, such as to whom the product is exported, and for what purpose. In that regard, the PROTECT Act also eliminates the end-user reporting that is so valuable to national security.

The PROTECT Act permits strong encryption products to be approved under a license exception or export to so-called "trustworthy" entities and regions without prior government knowledge of intended end-users. These include any foreign partners of U.S. companies, other governments, and almost any foreign commercial firm in any country. Some end-users could, in-fact, be targets of national security interest, such as narcotics traffickers. The PROTECT Act also automatically decontrols the export of strong encryption in the form of systems using the Advanced Encryption Standard (AES) systems to any destination, upon the adoption of AES, but at least by January 1, 2002. While current U.S. policy has opened up many sectors in many nations, it has done this in a thoughtful manner that minimizes the risk to important national security interests. The PROTECT Act could upset this delicate balance by widely expanding exports without due consideration to national security.

Finally, the PROTECT Act's 15-day technical review period is too rigid and too short to permit a meaningful technical review. The Government needs the opportunity to review a proposed export to assure it is compatible with U.S. national security interests and requires the ability to deny an export application if national security concerns are not adequately addressed. The ability to know what is being considered for export is a key part of U S. export control policy. In some cases today, this process takes longer than 15 days because insufficient information is provided as part of the initial application.

In summary, the PROTECT Act will harm national security by making NSA's job of providing vital intelligence to our leaders and military commanders difficult, if not impossible, thus putting our nation's security at some considerable risk. Our nation cannot have an effective decision-making process, a strong fighting force, a responsive law enforcement community, or a strong counterterrorism capability unless the intelligence information required to support them is available in time to make a difference. The nation needs a balanced encryption policy that allows U.S. industry to continue to be the world's technology leader, but that policy must also protect our national security interests.

Thank you for the opportunity to address the Committee.

Senator BURNS. Thank you.

I will start it off here. I just want to ask the Deputy Director, why is it that we have not been very successful in our negotiations with other countries to come up with some kind of international policy with regard to the use of or the export of robust encryption? In other words, we have been talking to our, I think he is related

to an ambassador, Aaron, and we have been told that countries are moving to export controls, especially in the European Union and around the country, of which no agreement to my knowledge and we have drawn no conclusions to move in that direction in the last 4 or 5 years ever since we have been doing this.

Ms. MCNAMARA. I believe we have had success in that, Mr. Chairman last December—well, let me begin by saying, last September the U.S. Government, the U.S. administration, relaxed export controls substantially, to include the 128-bit encryption that Senator Ashcroft was addressing earlier and to cover the firms in his home State that actually have locations overseas, to allow them to be able to use very strong encryption, 128-bit, to protect theirs.

Now, in December we took the U.S. policy to the Wassenaar countries. Those are 33 nations who are the principal producers of strong encryption around the world. That Arrangement—we took the U.S. relaxation strategy to that group of people and what we did at the time successfully was to close a loophole that the Wassenaar Arrangement had previously opened which was providing an unlevel playing field and disadvantaging U.S. software companies.

So last December we sought and got agreement by 33 nations to close that loophole. The Arrangement allows for all 33 of those nations to put in place, those who already did not have in place, export controls that are essentially the same level as the controls that the U.S. administration relaxed to last September.

With regard to what is going on in the European Union, we, the Administration—and I will turn this over to Secretary Reinsch to follow up on—but we are keeping our eye very closely on what is going on today in the European Union and what those foreign governments are thinking about in terms of encryption policies with regard to Europe. It is never our intent to allow anything to occur by foreign governments that would disadvantage U.S. industry.

Senator BURNS. Senator Ashcroft.

Senator ASHCROFT. Secretary Reinsch, would you say that 128-bit encryption is widely available and widely used today?

Mr. REINSCH. No, I would say that it is available. Whether it is widely available is a judgment call. If it is not widely available today, it will be soon. It is becoming the state-of-the-art, if you will, so I think it is a matter of time, and I would not have a big argument with you over the adjective.

Whether it is widely used or not is a more complicated question, and I think Ms. McNamara commented on that in her statement. We believe that, for the reasons she cited, use is significantly less than the existence of the products.

Senator ASHCROFT. Do you know of any case where there has been a prosecution or an enforcement action taken against people who have, or criminals who have used encryption outside the range of encryption that has been provided as acceptable? It would be an export, I guess, enforcement because the use would be a violation of the export regulations. Have you enforced this against anyone?

Mr. REINSCH. Yes, sir.

Senator ASHCROFT. How many cases have there been?

Mr. REINSCH. I will have to get you the number. We have a number of investigations ongoing, which of course we would not want

to comment on. We have had a number of—we will have to get you the number. I would say single digits at this point.

Senator ASHCROFT. But it is only illegal to export the encryption? It is not illegal to import the encryption?

Mr. REINSCH. That is correct, there are no restraints on domestic use or on imports.

Senator ASHCROFT. So that it is a one way? In other words, if terrorists conspire overseas to do something, like to effect a terrorist act here in the United States, they can send material in that is encrypted to the United States?

Mr. REINSCH. Well, we do not control in any event messages or information that is encrypted. What is controlled is the encryption that one would employ.

Senator ASHCROFT. Is the sending of an encrypted message from the United States to another jurisdiction, does that qualify as an export of the encryption?

Mr. REINSCH. No.

Senator ASHCROFT. It does not. So that—

Mr. REINSCH. Unless the message contains an encryption algorithm which is controlled. But if I sent—if you were in Bonn and I sent you an e-mail and it is encrypted, no.

Senator ASHCROFT. So it is true that the person or the terrorist organization which buys its encryption from Siemens in Germany can operate say in the Middle East and send messages back and forth to the United States, having imported the algorithm to the United States from Germany and have taken the German algorithm to the Middle East, and they can communicate back and forth without violating any of our laws currently?

Mr. REINSCH. Yes. There is no—it was never the intent of our policy to try to deal with that.

Senator ASHCROFT. Well, it seems to me that that is the threat that you keep saying that we are avoiding by having this policy, and yet you just described that it is not our intent to stop that threat with our policy. To use that as the basis for not allowing our companies to compete, at a time when you say we do not care if other companies compete in that way, gets to the heart of what confounds me about our policy here.

We have basically said every other country that wants to can go ahead and do this in the world and terrorists can use it and have complete access to the utilization of this encrypted for all the bad reasons, but American firms cannot be involved in exporting it. It just seems that is where the disconnect comes with this Senator and that is what I am struggling with.

You said that section 102 incentives—provides an incentive to move the development of encryption offshore in this bill.

Mr. REINSCH. Yes, sir.

Senator ASHCROFT. It seems to me that we have just described the Administration policy as a monumental incentive to move encryption offshore because we have indicated that offshore-produced encryption can be used both to send and receive robust encrypted material from the United States, to and from, without violating the policy or the law.

Mr. REINSCH. Well, if I may comment, you have gone to one of the core issues, and I think it is an important dialogue to have. Let me make a small point first and then the larger point.

On the small point, the difference between section 102 and our policy is that our policy now would not permit a company to transfer encryption technology or production technology or encryption algorithm overseas for production purposes. Section 102 would, and that is the distinction we are making.

But the larger point you are making is a more important one, and let me say two things about that, if I may. One is that I think that, as Director McNamara acknowledged in her testimony, this is not a policy and there probably is no policy that is going to be air-tight with respect to our ability to prevent the kinds of people you cited, terrorists in your example, from obtaining and using robust encryption.

We do not believe that we can deal with every situation. The goal of our policy is to try to promote use in the marketplace of products that are law enforcement and national security-friendly, recognizing that a determined, committed terrorist who wants to use encryption can find ways around such a policy. But we believe by making, if we can, through market forces, the market standard, if you will, products that are more friendly to the interests of my two colleagues, what we will do over time is have more people, including some of the people that you are talking about, using this kind of encryption, which gives us some advantages. That is not going to happen in every case. We do not believe we can make it happen in every case.

Now, the second point that relates to what you said is this question of foreign availability, and I would like to comment on that because you commented in your opening statement on this as well. I think what Director McNamara said was that we do not want foreign availability to be the sole criterion.

Let me say that if it were the sole criterion for export control policy, we would not have controls on machine tools, we would not have controls on biotoxins, we would not have controls on chemical weapons precursors, semiconductor manufacturing technology, or computers at virtually any level. There are very few technologies over which the United States has a monopoly any longer, and you are quite right in saying that encryption is not one of them, but neither are the ones that I have mentioned.

If we are going to say that foreign availability ought to be our single standard or it ought to be the dispositive standard, the net result of that is I am not going to have very much to do in my job. It is our belief that you need to balance foreign availability considerations, obviously, and we do weigh foreign availability in our judgments without question, and Director McNamara just commented on why this is a particular issue in the European Union case.

But at the end of the day—and the Congress has been telling me this for 12 months with respect to satellites, with respect to computers, with respect to machine tools, that foreign availability is not the last word on the subject. Now, I think that it is ironic, to say the least, if the Congress is going to turn around on encryption and say that foreign availability is the last word on the subject.

Ms. MCNAMARA. May I follow up, please? The fact that one terrorist is using strong encryption that they either bought in the United States and took overseas with them or bought in Europe and is using it to communicate with people in this country is not what is of concern to us. On an individual basis, the U.S. Government I believe is smart enough to figure out a way to solve that particular problem or address that particular problem.

What we are talking about here is the issue of putting in place legislation which would allow the ubiquitous use of encryption around the world, independent of individuals. We can always solve an individual problem with an individual solution. But the subject of ubiquitous encryption has dramatic impact on our ability to do our national security business, and let me offer, if the Senator wishes, a classified presentation on some of the subjects that I cannot address in this particular room.

Thank you.

Senator ASHCROFT. Mr. Chairman, may I just clarify an item or two?

Senator BURNS. You may.

Senator ASHCROFT. Because these remarks have been extensive.

Mr. REINSCH. Sorry about that.

Senator ASHCROFT. No, that is all right. I am pleased to have these remarks.

Mr. REINSCH. You wind me up and get me started. These things happen.

Senator ASHCROFT. Well, thank you. Especially when I think you are supporting my position, I welcome your remarks.

Mr. REINSCH. Then I misspoke. [Laughter.]

Senator ASHCROFT. The Director just indicated that a person could buy and take overseas robust encryption from the United States and use it overseas. Is that considered an export?

Mr. REINSCH. Yes, that would not be permitted.

Senator ASHCROFT. Well then, you disagree with her that a person can do that legally?

Ms. MCNAMARA. I did not say it was legal. I do not think we will ever prevent everybody from committing a crime.

Senator ASHCROFT. OK. Well, I thought we were—I would just like to indicate that I did not raise the issue of terrorists. I am not interested in protecting terrorists here. I am interested in protecting our industry. But every time I want to protect the industry, one of you guys brings out the terrorist card and you throw it on the table and you say: "We cannot protect America because there are these evil people out there that are going to encrypt messages."

So I am interested in protecting U.S. companies, and I am also interested in protecting individuals. I guess some time I would like to have an answer why big companies and big business should have better, a greater right to privacy than individuals should in this country, and that commercial speech should be entitled to more integrity and privacy than individual speech.

So the idea of ubiquitous encryption—which I am charmed by that phrase. I mean, I am going to try to use it as often as I can.

Ms. MCNAMARA. May I retract that from the record?

Senator ASHCROFT. I thought it might be a description of Senate speeches, but——[Laughter.]

I think ubiquitous encryption is probably what we are headed toward in the marketplace of the world, and I think it is likely to be based on software developed outside the United States if we make it impossible for our software producers to have robust encryption here, because I think people are going to prefer to have privacy in their communications. I think most of us do. Very few of us like the idea of our calls or our communications being intercepted.

We are aware of technology that makes heard those things which were not heard. A whisper is no longer a whisper; it can become a shout with the right listening device. What we once thought was a secure transmission is now available. We want, we yearn for security as individuals, and the idea somehow that big business is entitled to encryption and that individuals are not in their communication is one of the hurdles that we have to kind of come together on somehow to solve this problem.

Thank you, Mr. Chairman.

Senator BURNS. Senator Cleland, do you have a statement? I am sorry. We have had some arrivals here.

STATEMENT OF HON. MAX CLELAND, U.S. SENATOR FROM GEORGIA

Senator CLELAND. Mr. Chairman, I would just like my ubiquitous opening statement to be——

Ms. MCNAMARA. I think I am going to regret I ever used that term.

Senator CLELAND [continuing]. Submitted, without objection.

Senator BURNS. I want somebody to spell it.

Senator ASHCROFT. The National Spelling Bee concluded last week.

Senator CLELAND. Thank you all very much.

I am an old Army signal officer and I am a little bit familiar with encryption and the power of encryption, both for the good guys and the bad guys. Mr. Robinson, I would like for you to help me a little bit. I am just trying to learn some new terminology here about recovery. Apparently for law enforcement recovery is a key item, so nonrecoverable encryption becomes a problem.

Recovery of what? How can you recover something that is encrypted, or is that the issue itself?

Mr. ROBINSON. Well, I think it is, Senator, in a sense. What we are really interested in is maintaining our ability—when we have probable cause and we go to court and get an order for electronic surveillance through a careful process that Congress has set out—to overhear communications. If what we get at the end of the road is encrypted, unrecoverable gibberish, we have a serious law enforcement problem.

I think that is true also of stored electronic data. Increasingly, as people store their records in electronic form, on laptops and others, we can get a search warrant—and frankly, I agree with Senator Ashcroft. I think privacy interests are very, very important and I think people have a right to privacy. We are not looking for an opportunity to evade or invade individuals' or companies' rights to privacy, and that is why I said in my statement I think it is important to have robust encryption.

But in those situations in which we have probable cause and we have procedures whereby we can go to court and get a wiretap order, a search warrant, we are going to be substantially handicapped if we do not try to contribute to an infrastructure that allows us to get plaintext out of these materials. That is our objective.

The how is a technological question. As the chairman indicated, I think we need the resources to try to solve this problem of what do we do with encrypted evidence of criminal activity. We have got to solve that problem, and we hope that there will be an infrastructure, a contribution to an infrastructure, that will allow us to get plaintext when law enforcement needs to have it to prevent crimes from occurring, to investigate them, and then to put the evidence in.

So that is essentially our equity, I think, in this debate.

Senator CLELAND. Help me out a little bit here. If we ease up on controls regarding exports of software, encryption software, that expands the bits, namely expands I guess the capability of data or information being encrypted, if we ease up on controls that allow for those software packages which allow for expansion of the bits or expansion of encryption to be sold abroad, then what you are saying is that we might get that back as a pie in the face. In other words, we might get that back in a greater difficulty for law enforcement to "recover" information; is that what I am hearing you say?

Mr. ROBINSON. Yes, I think that is true.

Senator CLELAND. Ms. McNamara, in terms of the pie in the face for you, that would be the lesser ability to, shall we say, to use the terminology, recover, shall we say, intelligence to then pass on to our commanders in the field? That is what we are talking about?

Ms. MCNAMARA. That is an accurate characterization of the situation, Senator.

Senator CLELAND. Mr. Reinsch, it seems like to me that this dovetails somewhat into the issue that we are all struggling with. I am on the Governmental Affairs Committee and the Senate Armed Services Committee. We are struggling with the issue of American technology, sensitive American technology, winding up in the hands of others, the most recent example being the Chinese, not just the espionage of our nuclear secrets and missile technology, but some of the, shall we say, leaked technology on missile and satellite information that wound up in the hands of the Chinese.

I would say that I was one of those who supported the licensing of this kind of technology to move from the Commerce Department to the State Department. I guess I am glad to see your bona fide concern, I think, in the Commerce Department about easing up on export controls on this sensitive information or this sensitive encryption capability.

I gather that the Commerce Department is very sensitive to this, is that correct?

Mr. REINSCH. Yes, and we would also say we were very sensitive in the satellite case as well, as I think I did say before your subcommittee when that first came up.

But yes, the decisions we make—the export control system of the United States is based on, leaving aside short supply, which is not on the table, controlling exports for national security and foreign policy reasons. That is the filter through which every decision we make goes. One might agree or disagree with a particular decision, but clearly in this case national security is a paramount consideration for us.

Senator CLELAND. Mr. Robinson, could you share with me a little bit. Does the Justice Department have some role in being involved in improving the U.S. end user verification system for supercomputers and strong encryption products? Is that a role that you play?

Mr. ROBINSON. Not directly, we do not. We are obviously concerned about the extent to which these issues interface with our ability to do our job.

Mr. REINSCH. We do that, Senator.

Senator CLELAND. That is through you in the Commerce Department?

Mr. REINSCH. Yes, end user visits, which are both pre- and post—that is, we do some in advance of making the decision about a license because we want to check out the bona fides of the end user, and post because we want to see if the item actually went where it was supposed to go and if it is being used as it was intended—has been an important enforcement tool for us for decades.

It is not the only enforcement tool we use by any means, and it has its imperfections. It is also very expensive. I would say that in general Congress has been less than generous with the resources that it would take to do more.

We have also been handicapped, frankly, on computers in specific, by a congressional requirement that we visit every one of them. This has forced us, for example, to visit subsidiaries of American companies who are using them, banks, companies that bought one computer and then 6 months later bought a second one; we have had to visit them twice. It has prevented our agents from doing what they do best, which is figuring out what the risks are and spending their investigatorial time and talent on the places that problems.

We have had to check a lot that we think are not problems. When you see the report of our inspector general on this subject next week, I think that—I should not get into this in public, but I think that he will make a distinction between visits that are useful and visits that are not useful. We want to do more of the former.

Senator CLELAND. Thank you very much.

In closing out my questions, Mr. Chairman—I know I am out of time here—Ms. McNamara, I gather that your message to us is that we should tread very softly on this issue of encryption and opening up or loosening up export controls because it does involve sensitive issues of national security?

Ms. MCNAMARA. Yes, sir.

Senator CLELAND. Thank you, Mr. Chairman.

Senator BURNS. Thank you.

Senator Dorgan, you have just joined us. Do you have a small statement? I am going to turn the chairmanship over to Senator

Frist—I have got an 11 o'clock that is sort of very important to me—if you would agree to do that. We have got one more panel to go, by the way.

STATEMENT OF HON. BYRON L. DORGAN, U.S. SENATOR FROM NORTH DAKOTA

Senator DORGAN. Mr. Chairman, I came late and I have to leave in a moment because of some other hearings, but I just want to make in 30 seconds a comment about all of this. I, as you know, worked with you in the last Congress to try to resolve some of these issues. These are very difficult issues.

You raise questions that I think are very important questions. Yet the whole export control area is very difficult. What used to be a supercomputer is now a laptop, available to anybody, any time, anywhere in the world. So as we try to sift through all of these issues and consider national security concerns, we also have to deal with the reality of what is happening in the world.

My hope is that we can find a resolution that is a thoughtful resolution, protecting our national security interests and at the same time recognizing what is happening in the rest of the world.

I appreciate the attention Senator Burns has given to this over some long period of time, that this is not an easy issue, and he has spent a great deal of time on it.

So thank you very much.

Senator BURNS. Thank you, Senator.

Senator Frist, I am going to turn this over to you. I have an 11 o'clock. I have tried to wheedle out of that thing two or three times and I am not having any more luck now than I had yesterday.

STATEMENT OF HON. BILL FRIST, U.S. SENATOR FROM TENNESSEE

Senator FRIST [presiding]. Thank you, Mr. Chairman. Mr. Chairman before you leave, I would like unanimous consent to have my opening statement made a part of the record.

Senator BURNS. You are the chairman. You can do anything you want to.

Senator FRIST [presiding]. Thank you very much.

First of all, I thank all three of you for being here. I have got a couple of other questions that I would like to just run through.

Director McNamara, do the continued export restrictions on U.S. encryption products make sense when Wassenaar partners such as the U.K., France and Germany have established new policies encouraging their citizens to use strong encryption?

Ms. MCNAMARA. In terms of the strong use—the use of strong encryption by individual nations' citizens, we support strong use of encryption by U.S. citizens. We do believe that U.S. citizens are entitled to privacy for their own purposes.

In terms of the export controls, however, there are agreements and there is compatibility and comparability between those export conditions that the United States has with the European partners that you mentioned. Now, there are discussions going on in Europe today. We have our eye on that. But when we relaxed last September, the European nations along with other members of the Wassenaar nations aligned their overarching documentation that

their export control processes should be in line with ours now both in hardware and software.

Senator FRIST. Is progress being made there, if you look out?

Ms. MCNAMARA. Yes, yes. In terms of what we are looking at, we still have our eye on Europe. The Administration said last year when we did relax to those sectors and encryption bit lengths that we would review those again in September, and one of the ingredients in that review will clearly be what other foreign governments are doing.

Let me state, though, for the record again, earlier I think it was Senator Ashcroft who said that we had—or perhaps it was Congressman Goodlatte when he was talking—that we had relaxed, the relaxation included going from 40 bits to 56 bits. That is clearly true, but in all of the sector relief that was given last year there is no bit length, as Secretary Reinsch said. It is 128-bits for use in banking, finance, commerce—sorry, online commerce, because it was recognition that e-commerce was a very important thing for U.S. companies and individuals to be able to have access to. So there is a large portion of that which is covered by 128-bit encryption.

Senator FRIST. Fine.

Mr. Robinson, OECD, European Community; could you elaborate on our global partners' positions on recoverable encryption products and their regulations, and specifically address OECD as well as the European Community?

Mr. ROBINSON. I think I would defer to the Secretary to give you a better answer than I.

Mr. REINSCH. I can do that.

Senator FRIST. Mr. Secretary.

Mr. REINSCH. Ambassador Aaron, who is the President's special envoy on this subject, has spent a lot of time with OECD members, I believe virtually all of whom are also members of what is known as the Wassenaar Arrangement, which is a multilateral export control regime that controls encryption items multilaterally. There are 33 nations in that regime, including Russia, including the NATO members, including all of the EU members, and a number of others.

As Director McNamara has said and as I testified, we have had a good bit of success in that group harmonizing the export control policies of all 33 of those members. At the same time, the individual countries are developing encryption policies domestically, and they have wrestled with the same issues domestically that everybody else has wrestled with: Do we want to control imports, do we want to control domestic use, what do we want to permit to happen in our countries?

There is a trend, I think it is fair to say, within the EU, which is the first place it would begin after here, away from key recovery, certainly away from controls on domestic use and in favor of allowing people within each of these countries to use whatever they want. There is, then, a trend away from what I would refer to as key escrow or key recovery, the idea that people mandatorily would have to provide a spare key with some third party entity, government or nongovernment.

We have also taken the position that we do not want to do that as a mandatory step. We do see an environment for stored data in which people may want to do that voluntarily, and we have taken exceptions to provisions in some of the bills that we think would discourage it voluntarily.

Most of our trading partners, whether you say OECD or the Wassenaar members or NATO, however you define them, are moving away from that kind of government involvement in the domestic marketplace. But at the same time they are all, on the export front, as near as we can tell, acting in a way that is generally consistent both with Wassenaar and with what we are doing.

Senator FRIST. Good. When we talk about appropriate agencies or parties to serve as key recovery agents, help me. What sort of appropriate agents or parties would that be?

Mr. REINSCH. Well, mostly private parties, in fact I think exclusively private parties now. You need to think about it from the standpoint of another piece of this issue that is not on the table and should not be, which is the question of authentication and reliability for authentication. This is not a spare key issue, but it is a question of a public key infrastructure issue—if I want to send you a message, you want to have some certainty that the message you receive with my name on it came from me rather than from him or someone else, and I want to have some assurance that your response came from you and not someone who has intercepted it and is masquerading as you.

That demands some authenticity and some certification that your message came from you. What we envision and in fact what a number of States have already addressed in their legislation is regulating the private entities that will provide that authentication function. They will not keep spare keys, because the last thing you want for authentication purposes is a spare key.

But what is happening is that private parties are springing up that will provide essentially trust services and authentication services to warrant that my messages come from me and that you can have some confidence in that. In fact, I think there are probably some people in that business on one of the next panels, and you might want to pursue the technology with them.

Senator FRIST. Right. Any other comment on that, Mr. Robinson?

Mr. ROBINSON. No, Senator.

Senator FRIST. Mr. Secretary, on the issue of research and development on computer security, you are against NIST's doing that?

Mr. REINSCH. Not necessarily. I think Justice is.

Senator FRIST. Mr. Robinson.

Mr. ROBINSON. Well, we are concerned that law enforcement be able to try to develop the techniques necessary to get plaintext because, frankly, we are the ones who are going to have to use them and we need to have the capacity to do so. We think it is critical to public safety and effective law enforcement when we encounter encrypted evidence of criminal activities to be able to figure out a way to turn that into real information, whether it is an audible transmission or stored electronic data. Without that capacity, obviously encryption in the wrong hands, as many things, can be a powerful tool to prevent law enforcement from preventing crimes

and successfully investigating and prosecuting them. So that is a concern that we obviously have.

Senator FRIST. I guess then my question, and feel free to comment, is as we look at standardization of an advanced encryption system, whoever is doing that, if it is NIST, needs to be up to date with state-of-the-art right where we are. I guess it is not clear to me how if you put the research and the development in computer security with law enforcement, with the FBI, and then have NIST looking at the standardization, how they are really on top of things. Or is it both?

Mr. REINSCH. If I could comment, one of my regrets this morning, Dr. Frist, was that I did not have an opportunity to bring with me a full and complete statement of NIST's views on that question. If I may, I would like to have them—what I will suggest to them is they might get in touch with you directly, knowing of your interest in the issue.

They do what you are describing. They have an extensive computer security laboratory now. They have a lot of interaction with the private sector. They validate products that they test as a service to the private sector.

I believe their view is that if the Justice Department wants to take the activity on, provided for in this bill, that that would be all right. If the committee wants to assign it to them, I am sure they would defer to the committee's judgment.

But what I would prefer is to have them communicate with you directly.

Senator FRIST. Fine.

Mr. REINSCH. I will arrange that.

Senator FRIST. Good.

Well, thank you. We do have another panel. Would any of you like to make any closing statements at all?

[No response.]

Senator FRIST. Thank you very, very much. We appreciate your being with us, and we will ask the second panel to come forward.

I thank all three panelists for being with us. I will go ahead and do the introductions and then we will go in alphabetical order, I believe: Mr. David Aucsmith, Chief Security Architect, Intel Corporation; Mr. Jim Bidzos, Vice Chairman of the Board, Security Dynamics Technologies; and Professor Lance Hoffman, School of Engineering and Applied Science, Cyberspace Policy Institute.

Welcome to each of you, and let us begin with Doctor—Mr. Aucsmith.

STATEMENT OF DAVID AUCSMITH, CHIEF SECURITY ARCHITECT, INTEL CORPORATION

Mr. AUCSMITH. Thank you, Mr. Chairman, for this opportunity to talk to you this morning about the need for fundamental reform of America's encryption policy. I am pleased to appear today on behalf of the Business Software Alliance, which together with ACP has been in the forefront of efforts to persuade the Government to adopt a new U.S. encryption policy.

I am from Intel. Intel is the world's largest semiconductor manufacturer and a major supplier of information technology building blocks to the global computer and communications industry. We

provide our customers with chips, printed circuit boards, assemblies, software—all the ingredients that you typically think of that go into a personal computer, servers, and workstations.

Actually, my being here to speak on behalf of the Business Software Alliance should underscore the fact that encryption is both a software and a hardware issue. In fact, as a general note, 56-bit hardware products are currently excluded from the favorable treatment now given by the Administration. That applies only to software products.

In 1998 we employed more than 40,000 people in the United States. We are headquartered in Santa Clara, CA, but have significant manufacturing facilities in a number of States, including Arizona, New Mexico, Oregon, California, and Massachusetts.

We urge the committee to pass the PROTECT Act with further amendments that would make the bill more fully comport with technical and marketing realities. This morning I would like to briefly make five points which I believe should underpin our U.S. encryption policy.

First: In an Internet economy, encryption is essential to all businesses, not just encryption business. I want to emphasize this point. While private sector interest in encryption export reform is generally characterized in terms of the competitiveness of American encryption products abroad, it has become a much larger issue for all American businesses.

In this economy, every business is becoming an Internet business. It will affect all businesses. Cryptography has emerged as the essential building block for building trust in the open Internet. Without it, the hundreds of billions of dollars of e-commerce currently projected to occur by the year 2002 will be at risk.

Second: Encryption is vital to securing America's critical infrastructures. I participated in the Defense Science Board evaluation of America's critical infrastructures. We focused on the vulnerability of five critical infrastructures and concluded that encryption is absolutely essential in their protection.

The security of any network is only as good as its weakest link. All wires have two ends, if you will. America's infrastructures cannot be protected if they are networked, as they will be, with foreign infrastructures that use weak encryption. That is why permitting exports of strong encryption helps to promote the national security.

Third: The availability of encryption cannot be reasonably controlled. Cryptography is just mathematics. Information about cryptography is widely available from many sources and in many forms. It is the subject of numerous academic conferences. It is taught in universities throughout the world.

Moreover, while developing good algorithms is extremely difficult, if you will, rocket science, implementing them is relatively easy once someone has developed them.

Fourth: Government-required or mandated plaintext access will not work. While mandated plaintext access offers at first glance a solution to the Government's problems, it is not technically possible in most circumstances. It does not let law enforcement verify compliance with access requirements a priori and it does not give national security interests access to stored information.

There is practically no commercial reason for storing communications keys and I believe the need for key recovery of stored data is overstated. To be blunt, Intel as a corporation does not plan to sell products incorporating key recovery, nor does it expect to implement a key recovery system for its own use.

Fifth: The Government needs to find technological alternatives to meet its requirements for access to information. Intel agrees that access to data communications and stored data by law enforcement and intelligence communities is both legitimate and extremely important. Clearly, Congress needs to adequately fund the technical efforts of these agencies so they can meet the challenges of the next century.

Industry supports additional funding. Industry can also provide assistance and is willing to do so. BSA has advocated that the U.S. Government should work cooperatively with our Nation's hardware and software manufacturers to develop the technical know-how that they need. Technical innovation is predominantly centered in the private sector. Only a government-industry cooperative exchange can effectively address the challenge of continued technological change.

In conclusion, let me say that we strongly believe the PROTECT Act should be passed, but with further improvements. The PROTECT Act does not—I mean, the PROTECT Act does begin to realize the realities of mass market products. It eliminates reporting requirements for such products and grants export relief to those products at all horizontal layers of the information technology sector.

But the Act still does not grant widespread exportability of mass market and publicly available encryption products, and there is a complicated bureaucratic process which must be pursued. Not until 2002 will American industry be able to widely export products that are now using what is basically the worldwide standard of 128 bits in the form of the Advanced Encryption Standard or its equivalent. We believe that it is in our national interest to permit such exportability now and we urge the committee to amend the bill accordingly.

Thank you very much.

[The prepared statement of Mr. Aucsmith follows:]

PREPARED STATEMENT OF DAVID AUCSMITH, CHIEF SECURITY ARCHITECT, INTEL CORPORATION

Thank you Mr. Chairman for the opportunity to talk to you this morning about the need for fundamental reform of America's encryption policy. I am pleased to appear today on behalf of the Business Software Alliance which, together with ACP, has been in the forefront of efforts to persuade the U.S. Government to adopt a new U.S. encryption policy. We urge the Committee to pass the PROTECT Act with further amendments that would make the bill more fully comport with technological and market realities.

This morning I would like to briefly make five points that we believe should underpin U.S. encryption policy.

First, encryption is essential to all business in an Internet economy. While private sector interest in encryption export reform is generally characterized in terms of the competitiveness of American encryption products in a worldwide market, it is becoming a much larger issue for all American business. The global economy, tied together with the Internet, is turning businesses into virtual enterprises, localized products into global products, and geographically limited networks into worldwide networks. In this environment, American businesses must be able to sell and support their products worldwide, must be able to securely coordinate with their busi-

ness partners worldwide, and must be able to conduct safe electronic commerce worldwide.

Quite simply, cryptography has emerged as the only possible solution to many of the requirements of commercial security. It is the essential building block for building trust onto the open Internet. Without it, the hundreds of billions of dollars of e-commerce currently projected to occur by the year 2002 will not happen.

Second, encryption is vital to securing America's critical infrastructures. Much of the national economy is at risk from the decisions that are made today on the issues of infrastructure protection. Increasingly, these critical systems are driven by, and linked together with, computers making them vulnerable to disruption. The single best way, and sometimes the only way to affect effectively these critical networks and systems, is encryption. That's why the National Research Council found that encryption promotes the national security of the United States. However, the security of any network is only as good as its weakest link. America's infrastructures cannot be protected if they are networked with foreign infrastructures using weak encryption.

Third, the availability of encryption cannot be reasonably controlled. Cryptography is a branch of mathematics. Cryptographic technology can be reduced to mathematical formulas and protocols. Information about cryptography is available from many sources in many forms. It is the subject of numerous academic conferences. It is taught in universities worldwide. Moreover, while developing good algorithms is tough, implementing them is relatively easy.

Fourth, government promoted or required plaintext access will not work. While required plaintext access offers, at first glance, a solution to the government's problem: (1) it is not technically possible in most circumstances; (2) it does not let law enforcement verify compliance with access requirements; and (3) it does not give national security interests access to stored keys. There is simply no way that law enforcement can determine, in advance, that particular text had not been encrypted with more than one program or product. At the same time, targets of national security interests are unlikely to design or use a plaintext infrastructure which would allow the U.S. government to have secret access to plaintext.

Moreover, there is practically no commercial reason for storing communications keys—if the communication is disrupted or compromised a new session will be established. At the same time, the need for key recovery of stored data also is overstated—the frequent example is an employee hit by a bus. With the exception of personal notes, information is not solely possessed by an individual. In addition, most mission-critical data is held by the corporate data management system that has its own control and protection mechanism. Finally, most personal data has a time value and rapidly becomes obsolete.

If one factors in the additional costs and systemic vulnerabilities that result from building in access features, we conclude that there is no business or consumer need for key recovery or special plaintext access. To be blunt: Intel does not plan to implement a key recovery scheme for its own use. .

Fifth, the government needs to find technological alternatives to meet its requirements for access to information. Intel agrees that access to data communications and stored data by law enforcement intelligence communities is both legitimate and extremely important. Clearly, Congress should adequately fund the technical efforts of these agencies so they can meet the challenges of the next century. Industry supports additional funding. Industry can also provide other assistance.

For example, ACP proposed last year the creation of a "NET center" to help law enforcement officials understand how to deal with encryption and other technological advances. ACP also has advocated that the U.S. government should work cooperatively with our nation's hardware and software manufacturers to develop the technical tools and know-how that they need. Technical innovation is predominantly centered in the private sector—only a government/industry cooperative effort can address effectively the challenge of continued technological change.

In conclusion, let me say that we strongly believe the Protect Act should be passed but with further improvements.

The Protect Act does begin to realize the realities of mass market products, eliminates reporting requirements for such products, and grants export control relief to products at all horizontal layers in the information technology sector. But the Act still does not grant widespread exportability for mass market and publicly available encryption products. There is a complicated, bureaucratic process which must be pursued. Not until 2002 will American industry be able to widely export products using the 128-bit Advanced Encryption Standard or its equivalent.

We believe it is in our national interest to permit such exportability now and urge the Committee to amend the bill accordingly.

Once again, many thanks for this opportunity to testify.

INTRODUCTION

My name is David Aucsmith, and as Chief Security Architect for the Intel Corporation I am responsible for research, development and deployment of data and communications security technologies and products, both hardware and software. Currently, my work is focusing on developing industry standard architectures for the application and interoperability of data security technologies for communications, electronic commerce, and content protection. I previously worked on security matters for two computer companies and as a Lieutenant Commander in Naval Intelligence.

Intel is the world's largest semiconductor manufacturer and a major supplier of information technology building blocks to the global computer and communications industries. We provide our customers with chips, printed circuit board assemblies and software that are the "ingredients" of PC's, servers and workstations. Our flagship business involves the mass production and sale of the Pentium® family of processors and other microprocessors, which are frequently described as the "brains" of a computer because they control the central processing of data in computers. In 1998, our sales exceeded $26 billion, and we employed more than 40,000 people in the United States.

Like most information technology companies, Intel's business model is global in scope. The bulk of our production takes place in the United States. Our products are sold worldwide to original equipment manufacturers of computer systems and peripherals, PC users who make purchases through various distribution channels including the Internet, and other manufacturers who produce a wide range of industrial and telecommunications equipment. Information security plays a prominent role in the conduct of our business.

Intel is headquartered in Santa Clara, California, and we have significant manufacturing facilities in a number of states, including Arizona, New Mexico, Oregon, California and Massachusetts.

Intel Corporation is a member of the Business Software Alliance ("BSA") and Americans for Computer Privacy ("ACP"). Both associations have been in the forefront of efforts to persuade the government to adopt a new encryption policy.

Since 1988, BSA has been the voice of the world's leading software developers before governments and with consumers in the international marketplace. BSA promotes the continued growth of the software industry through its international public policy, education and enforcement program in 65 countries throughout North America, Europe, Asia and Latin America. Its members represent the fastest growing industry in the world. BSA worldwide members include Adobe, Attachmate, Autodesk, Bentley Systems, Corel Corporation, Lotus Development, Macromedia, Microsoft, Network Associates, Novell, Symantec and Visio. Additional members of BSA's Policy Council include Apple Computer, Compaq, Intuit, Sybase and my company Intel. BSA websites: *www.bsa.org; www.nopiracy.com.*

Intel Corporation takes, as a given, that access to data communications and stored data by the intelligence and law enforcement communities is both legitimate and extremely important. But, we also recognize that there is an inevitable tide of advancing technology that renders most conventional intercept methodologies obsolete. We also believe that all American businesses need access to strong cryptography to remain competitive in an ever increasing global economy.

We believe that these varied objectives can be met if only government does not seek to force solutions on industry that are incompatible with the development of technology and market demands. It is our view that, given the breathtaking pace at which information technology (including cryptography) is developing around the globe, the only way to achieve these goals is to adopt policies that will ensure American industry leadership in the area of information technology.

This morning I would like to discuss five points that we believe should underpin U.S. encryption policy:

1. Encryption is essential to conducting all business in an Internet economy;
2. Encryption is vital to securing America's critical infrastructures;
3. The availability of encryption cannot be reasonably controlled;
4. Government promoted or required plaintext access will not work; and
5. The government needs to find technological alternatives to meet its requirements for access to information.

ENCRYPTION IS ESSENTIAL TO CONDUCTING ALL BUSINESS IN AN INTERNET ECONOMY

While the private sector interest in encryption export reform is generally characterized in terms of the competitiveness of American encryption products in world markets, it is, in reality, a much larger issue for American businesses. In an Internet economy, all American businesses are affected by encryption export constraints.

The future of business is fundamentally changing. The Internet presents two distinctly different business opportunities.

• *Moving existing business to the Internet.* Taking our existing paper-based commerce models and moving them to the electronic world.

• *Creating new businesses because of the Internet.* The Internet provides a ubiquity, connectivity and speed that has never existed before. There are many hereto unimagined businesses that will arise to capitalize on these capabilities.

The global economy, tied together with the Internet, is turning businesses into virtual enterprises, localized products into global products, and geographically limited networks into worldwide networks. Taking place on a massive scale, this phenomenon rests on the following business principles:

• American businesses must be able to sell and support their products worldwide.

• American businesses must be able to securely communicate and coordinate with their foreign subsidiaries and business partners worldwide.

• American businesses must be able to conduct safe electronic commerce worldwide.

I will address each of these three principles in more detail. However, it should be obvious that they all depend on secure communications and financial infrastructures. Cryptography is an essential component of the security of these critical infrastructures, regardless of the nature of the company involved.

It is easy to underestimate the magnitude of the information technology industry in the U.S. and the importance of Internet driven electronic commerce. The Department of Commerce reported that:

Without information technology—and the electronic commerce it fosters— overall inflation would have hit 3.1% last year, more than a full percentage point higher than the 2% it was . . . [1]

By the year 2002, Internet commerce is expected to be $327 billion [2] annually. By the year 2001, the U.S. information technology industry will be directly responsible for 5% of the GNP.[3]

American businesses must be able to sell their products worldwide

Much has been said about the need for American businesses to be able to sell their encryption products worldwide as will be discussed later in this testimony. What is not obvious is that encryption controls may make it difficult to sell non-encryption products on the world market as well. For example, a telecommunications application may need to have an integrated cryptographic component to meet an international standard.

American businesses must be able to securely communicate and coordinate with their foreign subsidiaries and business partners worldwide

Business practices demand tight coordination with both a companies overseas subsidiaries, their suppliers and their customers. It is essential that confidentiality and access control to business information be maintained. Frequently companies are suppliers or customers on one product and competitors on another. The tightly integrated networks required for coordination could rapidly become a source of competitive intelligence if not adequately protected. Only strong cryptography can offer the level of protection required.

American businesses must be able to conduct safe electronic commerce worldwide

In the near future, there will now longer be dedicated Internet companies—virtually every company will have to be an Internet company to survive. This requires that companies have the capability to securely sell products over the Internet to markets around the world. The ability to prevent fraud and protect intellectual property will depend heavily on the use of strong cryptography.

Importantly, corporate participation in electronic commerce includes both business-to-business and business-to-consumer transactions.

There is a need for commercial security

There has always been some level of need for data security in commercial environments. However, the Internet has enabled the connected PC and, with it, created both new business opportunities and new security vulnerabilities.

Both the value and volume of on-line information has sharply risen. This information includes organizational information such as financial data, manufacturing information, customer information, medical and legal records, and human resources data. Additionally, there is a growing amount of data which has intrinsic value, such as monetary instruments (e.g., credit cards, coupons, etc.) and intellectual property (e.g., movies, images, etc.).

In the past, such data was protected by physical and procedural controls. The connected PC largely negates those conventional controls and requires new security mechanisms, thus creating a need for commercial security technology.

After many years of false starts, commercial data security has become a viable business. The Internet has provided the driving force for this change. Physical barriers have all but disappeared, and security perimeters have become vague.

The Internet has created needs for security that were not present in isolated security domains. This has, in turn, created opportunities for vendors of security technologies and has also created a need for standards so those technologies can interoperate.

Cryptography is the only viable solution to most commercial security requirements

Cryptography has emerged as the only possible solution to many of the requirements of commercial security. It is the essential building block for projecting trust onto the open Internet.

The modern global commercial information infrastructure is characterized by more than 95 million Internet-connected computers,[4] most of which are in open environments with little or no physical control. They use a wide variety of hardware and software and implement no common security policy.

Only cryptographic technologies are capable of projecting security onto a completely open, arbitrary environment. Cryptography, by itself, does not guarantee any level of security. It is a necessary component but not a sufficient component.

Privacy, also known as confidentiality, is the characteristic that information is protected from being viewed in transit during communications and/or when stored in an information system. With cryptographically-provided confidentiality, encrypted information can fall into the hands of someone not authorized to view it without being compromised. It is almost entirely the confidentiality aspect of cryptography that has posed public policy dilemmas.

The commercial use of privacy (or confidentiality) encompasses not only the traditional view described above, but also the protection of intellectual property such as digital video and digital audio. The same technology used to keep communications private are required to ensure that a digital movie is not illegally copied.

ENCRYPTION IS VITAL TO SECURING AMERICA'S CRITICAL INFRASTRUCTURES

Governments also are recognizing that without encryption, the electronic networks that control such critical functions as airline flights, health care functions, electrical power and financial markets remain highly vulnerable. The U.S. General Accounting Office in its report issued in May of 1996 entitled "Information Security: Computer Attacks at Department of Defense Pose Increasing Risks" found that computer attacks are an increasing threat, particularly through connections on the Internet, such attacks are costly and damaging, and such attacks on Defense and other U.S. computer systems pose a serious threat to national security.

There is an awareness within the government of the vulnerability of the national information infrastructure to potential attack. The Marsh Report[5] highlighted the vulnerabilities very well. Much of the national economy is at risk from the decisions that are made today on the issues of infrastructure protection. Any action that degrades the security of Internet commerce or the viability of the industries involved must be viewed as a serious risk to the national security.

As the President said on January 22, 1999, before the National Academy of Sciences, "[w]e must be ready—ready if our adversaries try to use computers to disable-power grids, banking, communications and transportation networks, police, fire and health services—or military assets. More and more, these critical systems are driven by, and linked together with, computers, making them more vulnerable to disruption."

The President has been so concerned that he established a Commission on Critical Infrastructure Protection to provide him with guidance and issued two Presidential Directives based on the Commission's recommendations.

In the Report of the President's Commission on Critical Infrastructure Protection entitled Critical Foundations: Protecting America's Infrastructures (October 1997), the Commission emphasized that "Strong encryption is an essential element for the security of the information on which critical infrastructures depend." In fact "[p]rotection of the information our critical infrastructures are increasingly dependent upon is in the national interest and essential to their evolution and full use. A secure infrastructure requires the following:

- Secure and reliable telecommunications networks.
- Effective means for protecting the information systems attached to those networks . . ..
- Effective means of protecting data against unauthorized use or disclosure.

• Well-trained users who understand how to protect their systems and data."

An earlier blue ribbon National Research Council (NRC) Committee similarly concluded in its (May 1996) CRISIS Report ("Cryptography's Role in Securing the Information Society") that encryption *promotes* the national security of the United States by protecting "nationally critical information systems and networks against unauthorized penetration."

Thus, the NRC Committee found that on balance the advantages of widespread encryption use 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."

In recognition of the risks and threats to information, on January 15, 1999, the National Institute of Standards and Technology (NIST) established a new draft Federal Information Processing Standard (FIPS 46–3) to require the use of stronger encryption in government systems. NIST stated that it "can no longer support the use of the DES for many applications" and that all new systems must use the significantly stronger Triple DES "to protect sensitive, unclassified data". Under the FIPS, all existing systems are now expected to develop a strategy to transition to Triple DES, with critical systems receiving a priority.

The vulnerability of national infrastructures has not been lost on other governments. Within the European Union, there is discussion on how to encourage companies to develop products to protect national infrastructures in their respective countries. Such mutual government encouragement will help to grow technical capabilities and fuel a viable world market.

Already the Swiss government is providing 128-bit encryption plug-ins for download off the Internet. The SecureNet system is required for use in accessing Telegiro, an Internet payment system. The plug-ins support SSL connections using IDEA encryption. Several Swiss banks are now using on-line banking systems compatible with the Telegiro cryptosystem.[6]

Information security is critical to the integrity, stability and health of individuals, corporations and governments. While cryptography is but one element of security, it is the keystone of secure, distributed systems. Frankly, there is no substitute for good, widespread, strong cryptography when attempting to prevent crime and sabotage through these networks. The security of any network, however, is only as good as its weakest link. America's infrastructures cannot be protected if they are networked with foreign infrastructures using weak encryption.

In the long-term, we believe it is in America's best interest to protect critical infrastructures and national security by relying on strong American encryption products. This will not happen if the U.S. Government limits the ability of U.S. companies to provide strong encryption to consumers. Indeed, the question is not whether critical infrastructures will be protected. Rather it is a question of who will protect them—U.S. or foreign companies. With individuals increasingly relying on critical infrastructures and governments increasingly desiring to safeguard these infrastructures, it is only a matter of time before strong encryption becomes a commodity feature of global networks and information systems.

U.S. encryption export controls hurt our national security

Our current export policy puts at risk America's global leadership in information security. U.S. export policy should, therefore, be changed so it no longer limits American participation in efforts to secure global e-commerce and related information infrastructures and no longer cedes the world market for encryption products to foreign competitors. Strong, high-quality encryption products already are widely available from foreign makers. Foreign producers of IT systems are finding that their ability to provide end-to-end systems incorporating stronger encryption than U.S. companies are permitted to export gives them a decided market advantage. We are concerned that as a result America will lose the critical encryption market to foreign companies. If that happens, it will be too late to change U.S. policy and too late to preserve U.S. leadership in this vital arena.

What will the loss of that U.S. leadership position mean? It will mean that the national security agencies will be confronting ubiquitous encryption made not by U.S. companies, but by foreign companies. Where then will the national security agencies go for technical help on encryption? It also will mean that the protection of our critical national infrastructure may depend on foreign-made systems incorporating foreign-made encryption—and that's unacceptable.

America must retain leadership in this vital technology if we are to meet our long-term national security objectives. That is why we must assess our encryption export policies from a long-term, not a short-term, perspective.

In the long run, U.S. national security objectives are best served by an IT world in which U.S. companies are market leaders in all aspects, especially encryption. U.S. export controls have had the effect of creating an encryption expertise outside the United States that is gathering momentum. Unfortunately, every time research and development of an encryption technique or product moves off-shore, U.S. law enforcement and national security agencies lose. We believe that continuing down this path will be ultimately more harmful to our national security and law enforcement efforts as American companies will no longer be the world leaders in creating and developing encryption products.

In fact, as long ago as 1996, the NRC Committee concluded that as demand for products with encryption capabilities grows worldwide, foreign competition could emerge at levels significant enough to damage the present U.S. world leadership in information technology products. The Committee felt it was important to ensure the continued economic growth and leadership of key U.S. industries and businesses in an increasingly global economy, including American computer, software and communications companies. Correspondingly, the Committee called for immediate and easy exportability of products meeting general commercial requirements—which is currently 128-bit level encryption!

We recognize this is a difficult balance to strike, but we strongly believe that our long term national security objectives can only be achieved if the United States realistically acknowledges the inevitability of a world of ubiquitous, strong encryption. Trying to control the proliferation of encryption is like trying to control the proliferation of mathematics. For that is what we are talking about here. Encryption algorithms are nothing but sophisticated mathematics. And while the United States may realistically hope to remain the leader in such a field, it cannot realistically expect to monopolize it.

We are joined in this view by the Center for Strategic and International Studies ("CSIS"). CSIS recently conducted a study of our nation's technical vulnerabilities; the study was chaired by William Webster, the former director of the FBI and Central Intelligence and former U.S. Circuit Judge. The subsequent report, entitled Cybercrime . . . Cyberterrorism . . . Cyberwarfare . . . Averting an Electronic Waterloo, calls for the "intelligence gathering communities—law enforcement and foreign intelligence—to examine the implications of the emerging environment and alter their traditional sources and means to address the SIW (strategic information warfare) needs of the twenty-first century. Continued reliance on limited availability of strong encryption without the development of alternative sources and means will seriously harm law enforcement and national security."

THE AVAILABILITY OF ENCRYPTION CANNOT BE REASONABLY CONTROLLED.

Cryptography is a specialized branch of mathematics. Cryptographic technology can be reduced to mathematical formulas and protocols. Information about cryptography is available from many sources and in many forms. Implementation of cryptography is no more difficult than the implementation of any complicated mathematical technology such as digital video or digital signal processing.

Ease of implementation

Creation of good cryptographic algorithms that will withstand the test of time is amazingly difficult. Recent history is littered with failed attempts. Even so, many algorithms have survived and have become part of common usage. Inventing good cryptography is the mathematical equivalent of "rocket science." Implementing those algorithms is comparably "child's play."

Information security is such an important part of information technology that it is rare for a graduate level computer science student to graduate without having implemented a cryptographic algorithm or protocol. Many of these students become competent systems-level programmers who could easily fashion a production-quality cryptographic application. Many of these students are non-U.S. residents.

Open research

Cryptography and cryptanalysis are legitimate academic research topics. There is a growing, worldwide academic community specializing in the subject. Last year alone there were over 30 international conferences focusing on cryptography or related topics and over 100 books and journals. Many of these books include detailed specifications and source code of cryptography algorithms and protocols.[7] As an example, Bruce Schneier's popular cryptography text, Applied Cryptography, has sold over 100,000 copies world wide.[8]

Intangible software

The intangible nature of cryptographic software defies any physical controls. In an instant, software, cryptographic or otherwise, can be shipped virtually anywhere in the world. As an example, within hours of the U.S. release of PGP 5.0, it was available from sites in Western Europe.[9]

Cryptography exists in many uncontrollable forms, such as general knowledge, academic research, and network deliverable software.

Availability of strong encryption products abroad

Having export controls assumes that they are at least marginally effective. Cryptography is basically mathematics. The knowledge is inherently uncontrollable. This has led to the worldwide availability of strong encryption products and technologies.

One of the ironies of the U.S. cryptographic export regime is that it has fostered a growth in non-U.S. cryptographic technology providers who can sell strong cryptography worldwide without the constraints imposed by the U.S. government, while U.S. companies can not make the same claim.

The belief that U.S. export regulations enable foreign cryptography businesses is held by the European Commission. The EC stated at the Copenhagen Hearing:

The current U.S. export regulations can provide a chance for European companies to enter the market for cryptographic products. Nevertheless this would require a concentrated effort of European industry and governments to prepare the basis for this market.[10]

Some European companies and governments have turned this belief into practice. The following is quoted from a Siemens Nixdorf ad regarding a software product of theirs called TrustedWeb:

By simply downloading the TrustedWeb software from the Internet, you can create a highly secure Intranet infrastructure in a matter of days. The organization itself can decide on the level of security and adapt it in stages in line with needs—Ranging from simple password protection to authentication using cryptographic procedures (Public Key/Private Key) with full 128-bit key length. TrustedWeb is an independent European product and hence is not subject to the export restriction imposed by the US government in relation to encryption software.[11]

Siemens Nixdorf runs similar ads covering their hardware products. Security products are available worldwide, in spite of, or perhaps because of, strong U.S. export controls.

Wide deployment of strong encryption is inevitable

There are huge commercial incentives for the spread of cryptography. There is a legitimate need for the technology and a sharp increase in the amount of money being spent on security technology.[12] This has created a viable market for the technology, and there are many suppliers worldwide willing and able to meet the market demand.

The recognition of the importance of security to data communications has lead to the inclusion of security protocols within international standards. Examples of such standards include the Secure Sockets Layer (SSL) and the Internet Packet Security (IPSEC) protocols.

In most cases, the implementation of security components in international standards is optional. However, there is a strong trend to make many of these features mandatory. Thus, compliance with international communications standards will promote the diffusion of security technologies.

GOVERNMENT PROMOTED OR REQUIRED PLAINTEXT ACCESS WILL NOT WORK

As the spread of strong cryptography threatens traditional intelligence methods, the government has used export control relief as an incentive for companies to build plaintext access capability into every product. There have also been attempts in Congress to mandate plaintext access capability in such products. The overall approach has revolved largely, though not exclusively, around key recovery requirements. This section primarily addresses specific concerns about key recovery issues, but it is applicable to all plaintext access solutions that may be promoted or mandated by the U.S. Government (hereinafter referred to as "required plaintext access"). The basic point is that non-market driven requirements to build any plaintext access mechanism into products will not work.

Key recovery, as a concept, now applies not only to the initial purpose of assuring law enforcement access to encrypted materials, but also to possible end-user or organizational requirements for a mechanism to protect against lost, corrupted, or unavailable keys. It can also mean that some process, such as authority to decrypt a header containing a session key, is escrowed with a trusted party, or it can mean that a corporation or individual is ready to cooperate with law enforcement to access

encrypted materials. It may also mean that some technical mechanism must be put in place to bypass the use of the key entirely (strict "plaintext access").

While required plaintext access offers, at first glance, the promises of solving the technical problems of plaintext access, it is not technically possible for it to do so in most circumstances. It is unlikely to actually meet plaintext access requirements, and its deployment as a national strategy is fraught with technical challenges and dangers.

Required plaintext access systems will not satisfy government access requirements

Required plaintext access does not meet either law enforcement or national security requirements, but for slightly different reasons. Law enforcement can not verify compliance with key recovery requirements, and national security interests are unlikely to have access to stored keys.

Compliance can not be verified by law enforcement

Required plaintext access has a serious technical flaw in the area of a priori verification of compliance. Encryption, if applied, is likely to be applied at several different levels of the communications infrastructure. An example is having link-level encryption applied by IPSEC, having session-level encryption applied by SSL, and having application-level encryption applied by S/MIME.

Assuming one could construct a protocol to allow for the monitoring of IPSEC key recovery compliance, there is no physical way to verify that the other two levels have complied with the required plaintext access requirements unless one actually decrypts the IPSEC-data packet. If it requires probable cause to get a court order to obtain the IPSEC recovered key or mechanism, it would only be after law enforcement has probable cause of criminal activity that they would be able to verify whether or not the upper-level protocols have complied with the required plaintext access requirements.

Required plaintext access does not address national security requirements

While law enforcement may serve a warrant on a key recovery agent or other access mechanism provider to obtain encryption keys or the plaintext, national security interests are likely to have that opportunity. Required plaintext access does not provide any benefit to lawful access unless one is able to actually recover the plaintext. Targets of national security interests are unlikely to design a plaintext access infrastructure which would allow the U.S. government to have surreptitious access to stored keys or stored plaintext. This view has been born out by National Security Agency testimony before Congress.[13]

Required plaintext access systems are of limited commercial value

Product announcements of key recovery companies to the contrary, there is not a compelling market for commercial key recovery systems and no market for other plaintext access systems. There is no general reason to recover communications keys, and the use of key recovery for stored data ignores the fundamental properties of information.

A market for key recovery technology will emerge only when it is artificially created by government regulations. Prior to the current law enforcement push for key recovery, there were no widespread deployments of key recovery mechanisms even though the basic technology had been in existence for some time.

Not required for data communications

While key recovery may, debatably, be important in certain stored data systems, in communications cryptography there is little or no user demand for this feature. In particular, there is hardly ever a reason for an encryption user to want to recover the key used to protect a communication session such as a telephone call, FAX transmission, or Internet link. If such a key is lost, corrupted, or otherwise becomes unavailable, the problem can be detected immediately and a new key negotiated.[14] There is also no reason to trust another party with such a key.

Ignores the nature of stored data

Many of the proposed needs for key recovery of stored data operate under a false assumption about how data is actually stored and utilized. The frequent example is the assertion that a company will need to recover the encrypted files of an employee who has been hit by a bus.

There are three problems with this assertion. First, with the exception of personal notes, information is not solely possessed by an individual. Information is shared among a team of employees or partners in order to be of any benefit. Second, most mission-critical data is held by corporate data management systems (e.g., data bases) that have their own access control and protection mechanisms, which are ad-

ministered by the corporation. Third, most personal data has a time value and rapidly becomes obsolete.

Given the observations above, we conclude that there is no business or consumer need for key recovery. Indeed, taking into account the observations and risks, Intel does not plan to implement a key recovery scheme.

Key recovery introduces additional vulnerabilities

Centralizing all of a user's secrets or access controls in a system with increased technological and procedural operational complexities can only increase the security vulnerabilities of the operation.

Centralized attack point

Regardless of the implementation, if key recovery systems must provide timely law enforcement access to a whole key or to plaintext, they present a new and fast path to the recovery of data that never existed before.

The key recovery access path is completely out of the control of the user. In fact, this path to lawful access is specifically designed to be concealed from the encryption user, removing one of the fundamental safeguards against the mistaken or fraudulent release of keys.

In contrast, non-recoverable systems can usually be designed securely without any alternative paths. Alternative paths to access are neither required for ordinary operation nor desirable in many applications for many users.[15]

Complexity of implementation

Key recovery systems must be, in terms of functionally, a secure, distributed, open key management system. They have many of the properties of both large scale distributed databases and of command and control systems. Both types of systems have significant inherent complexity. As we have no practical experience, key recovery mechanisms represent a system of unknown and potentially daunting complexity.[16]

Commercial organizations would have to add the cost and risk of key recovery systems to their bottom line. Even government agencies participating in key recovery pilot programs have found the cost of centralized key recovery unacceptable.[17]

Key recovery mechanisms do not work in the horizontal information industry

The information technology industry is characterized by an open, international, horizontal architecture. Microprocessors are sold to OEMs who build motherboards, who then contract to have BIOSs and operating systems installed. The final product is then sold to an end user who adds whatever applications they wish. New capabilities or requirements must have an active acceptance within each of the layers in order to be widely deployed. Key recovery discussion has focused only on the upper, application layer.

Low-level layers have no visibility into higher-level layers

The nature of the information technology industry is that it is made-up of distinct horizontal architectural layers, from the microprocessor up through application programs. The components in each of these layers are supplied by different companies, having different economic models and different diffusion channels.

For valid security reasons, cryptography is migrating further "down" the layers toward the basic hardware. Key recovery, on the other hand, is a user-initiated protocol problem and can not be pushed down to the hardware. In short, cryptography implemented on hardware can not determine how it will ultimately be used.

Key recovery is under the end user's control and is performed by communications protocols or applications programs. The original microprocessor could have no knowledge of how its cryptography would be used any more than it could know how its multiplication instructions will be used.

Key recovery regulation is envisioned from the perspective of the end user. The end user "sees" a vertical single product, but the reality is that the PC is actually a collection of products from many different companies.

Horizontal interfaces are international standards

Within the horizontal architecture of the computer industry, the interfaces between horizontal layers are defined by established international industry standards. None of these interface standards currently support key recovery of keys stored in mass market hardware. To change these standards would be a slow and difficult process.

Key recovery does not work in an international setting

The information technology industry is based on international standards. No U.S.-only solution is commercially feasible. Most U.S. information technology companies

derive a large share of their revenue from non-U.S. sources. To restrict their products to only U.S. markets would be devastating.

Not all countries will adopt key recovery

Very few countries have embraced key recovery to the extent that the U.S. government has done. In particular, countries with strong privacy laws have generally regarded key recovery schemes as being in violation of those laws. As an example, Lotus Notes, which includes a key recovery feature, specifically lost a major sale to the Government of Sweden when the Swedish press discovered the key recovery feature.[18]

The European Commission has not endorsed key recovery as a solution to lawful access problems. It is therefore unlikely that a European-wide agreement can be reached. Indeed, the European Committee on Banking Standards (ECBS)—a powerful consortium of financial institutions—has filed a submission with the European Commission arguing against key recovery.[19]

Requires modification to existing standards

Data communications and architectural standards are internationally-negotiated standards. None of these standards include data recovery provisions. Products must be built to conform to these standards to become mass market products. Many of these standards are not controlled by any government, rather they are controlled by commercial or user communities (such as the IETF).

Negotiating provisions for key recovery into these standards will require international—agreement on the form and procedures of key recovery technology. Given the current international climate, it is unlikely that such negotiations would succeed.[14]

Interoperability will require a non-recovery mode

If there is even one major country which prohibits key recovery, then all developed systems will have to have a "non-key recovery" mode to facilitate interoperability. There is little that one could do to ensure that the "non-key recovery" mode was not used in normal communications.

Mutual access to keys opens U.S. companies to industrial espionage

There is no way to guarantee that other countries will have the same level of constitutional safeguards on access to their key recovery agents as guaranteed in the U.S. U.S. corporations would be at high risk of international economic espionage if forced to deposit encryption keys with foreign key recovery agents.

According to the FBI, U.S. corporations are already targets of major industrial espionage efforts. The FBI says foreign spies have stepped up their attacks on American companies, and a new national survey estimates that intellectual property losses from foreign and domestic espionage may have exceeded $300 billion in 1997 alone.[20]

Governments of at least 23 countries, ranging from Germany to China, are targeting American companies, according to the FBI. More than 1,100 documented incidents of economic espionage and an additional 550 suspected incidents that could not be fully documented were reported last year by companies in a survey conducted by the American Society for Industrial Security.[21]

THE GOVERNMENT NEEDS TO FIND TECHNOLOGICAL ALTERNATIVES TO MEET ITS REQUIREMENTS FOR ACCESS TO INFORMATION

Given the global availability of strong, non-recoverable encryption and the fast pace of technological advancement, it is clear that current U.S. policy is not working. An alternative means to gather lawful intelligence is needed by both national security and law enforcement interests.

Clearly, Congress should adequately fund the technical efforts of our law enforcement and national security agencies so they can meet these challenges. And industry would support additional funding.

For example, ACP, for example, has advocated that the U.S. Government should work cooperatively with our nation's hardware and software manufacturers to develop the technical tools and know-how to achieve a policy that effectively responds to society's needs for law enforcement, national security, critical infrastructure protection, privacy preservation, and economic well-being.

NET center proposal

Last year, ACP proposed the creation of a National Center for Secure Network Communications ("NET Center"). The NET Center (now called "Tech Center") concept is 15 aimed at helping law enforcement officials to understand how to deal with encryption and other technical advances when encountered in a criminal setting.

The Tech Center should be a public-private entity operating within a national laboratory for information technology to perform research and act as a forum for further discussions on technology trends and vulnerabilities. Clearly a Tech Center must operate within a legal framework that provides reasonable safeguards.

Attorney General Janet Reno announced plans for the Federal Bureau of Investigation to set up a new $64 million center to protect the nation's critical infrastructures, particularly computer networks, from both physical and cyber attack.

Industry cooperation

The national security is best secured by the American companies actively competing for and supplying the fundamental technologies of the national infrastructure. Only those companies directly involved in the research and development of information technology components can assess the security and vulnerabilities of the infrastructures created from those components. Technical innovation is predominantly centered in the private sector. Only a government/industry cooperation can effectively address the challenge of continued technological change.

CONCLUSION: THE PROTECT ACT SHOULD BE PASSED WITH FURTHER IMPROVEMENTS

The mass market model

Mass-market hardware manufacturers and software publishers sell products through 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. Thus, mass market products are available to the general public from a variety of sources.

The mass-market distribution model presupposes that hardware manufacturers and 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. As mass market products are uncontrollable, Intel believes U.S. companies should be able to export the current market standard of 128-bit encryption. Unfortunately, the Administration only permits easy exports of 56-bit encryption even if foreign products exist in the marketplace'. And the Administration continues to impose onerous controls on 56-bit toolkits and hardware encryption components, notably semiconductors.

The PROTECT Act grants export control relief to products at all horizontal levels

Intel believes that all distinct horizontal architectural layers, from the microprocessor up through application programs should be treated identically under any encryption export policy. However, contrary to the Administration's original announcement regarding export relief which included export relief for hardware, the new regulations still do not permit 56-bit encryption chips, integrated circuits, toolkits and executable or linkable modules to be easily exported except to subsidiaries of U.S. companies or otherwise relax export controls on stronger mass market hardware. We are pleased that the PROTECT Act remedies this problem and treats mass market hardware in the same manner as mass market software.

The PROTECT Act eliminates reporting requirements for mass market products

We are encouraged that the PROTECT Act recognizes the difficulties in complying with reporting requirements for mass market encryption products and eliminates such reporting requirements. It is virtually impossible for mass-market exporters to report the name and address of each end-user. Millions of these products are sold through multi-level distribution channels (e.g, VAR's and chain stores). Moreover, as registration of mass market products is customarily voluntary. This is a vast improvement over the Administration's proposed regulations which effectively require companies to develop a system to obtain the names and addresses for each health and medical end-user of stronger encryption products and all foreign online merchants.

The PROTECT Act's export relief for mass market products and for products which face competition from comparable foreign products is too complicated and creates an unwieldy bureaucracy

We are pleased that the PROTECT Act does recognize that mass market and publicly available encryption products, and encryption products for which comparable foreign products are available, should be treated differently under the U.S. export regime. The bill acknowledges the futility of trying to control a product that can be bought off of the Internet or easily purchased from commercial vendors such as CompUSA or from Circuit City by any individual in America regardless of nationality, or a comparable product can be easily purchased from similar stores in a for-

eign country. "Bad guys" certainly will have no problems obtaining the encryption products, and no concerns about "exporting" the products via telephone lines or the Internet or smuggled out on personally pressed CDs. The only impact of the export controls will be to stop American companies from selling American products to legitimate users.

Unfortunately, the PROTECT Act establishes a complicated private/public board structure for deciding after-the-fact whether or not a product is a mass market product or whether comparable foreign products are available. The Secretary of Commerce has thirty days to approve or disapprove the Board determination, subject to judicial review, and the President may override any determination. There is no guarantee of any consistency in the Board's decisions. Thus, while the Board procedure is an improvement, and the opportunity for judicial review provides a mechanism to ensure that exports are not denied in an arbitrary and capricious manner, it is not a predictable, clear process giving American companies certainty as to whether they can export their products. Such predictability is necessary so that American companies can have confidence designing and building security features into their products.

The PROTECT Act should, but does not, afford complete and immediate export relief for mass market encryption without any complicated oversight. The Act also does not recognize that if a comparable foreign product is available, any delay in exports provides a significant advantage to the foreign product.

The PROTECT Act supports development of AES, but delays full export control relief until 2002

The PROTECT Act also provides Congressional support for, and sets a 5-year limit on the selection of, the 128-bit Advanced Encryption Standard which is being developed under the auspices of the National Institute of Standards and Technology. The 2002 deadline will provide impetus for NIST to finish developing the standard in a timely manner while providing NIST with sufficient time to study the final standard's security features. This is an important process that will result in a new standard for government's sensitive, but unclassified, information and most likely will serve as the new worldwide standard for strong encryption similar to the Data Encryption Standard when it was introduced in the 1970's. Once the algorithm is selected, the PROTECT Act removes all export controls on encryption products using the 128-bit standard or its equivalent strength.

Unfortunately, because the PROTECT Act limits easy exportability of mass market products until the AES is adopted, general distribution of these products will have to wait almost three years. Considering the current speed of technological change, where Internet products are now on three-month product cycle times, and the fact that 128-bit comparable foreign encryption is currently available, this is an eternity in Internet time. Law enforcement and national security interests have known for a long time that ubiquitous use of strong encryption by consumers worldwide is just around the corner. They cannot hope to continue to delay the world from using strong encryption according to their timeframe.

A new approach

The preceding has made the argument that:

- Encryption is essential to conducting all business in an Internet economy;
- Encryption is vital to securing America's critical infrastructures;
- The availability of encryption cannot be reasonably controlled;
- Government promoted or required plaintext access will not work; and
- The government needs to find technological alternatives to meet its requirements for access to information.

If accepted, these arguments force one to the conclusion that a new approach to encryption policy is required.

ENDNOTES

[1] Wall Street Journal, Department of Commerce talks about Inflation, 16 April 1998.

[2] Forrester Research

[3] Dataquest

[4] Ibid., p. 8.

[5] Marsh, R., Chairman, Critical Foundations: Protecting America's Infrastructure, The President's Commission on Critical Infrastructure Protection, October 1997.

[6] See http://www.swisspost.ch/E/21.html

[7] Schneier, B., Applied Cryptography, John Wiley & Sons, Inc., New York, NY, 1996.

[8] Schneier, B., Private correspondence, June 1998.

[9] Hayward, D., Europeans Break Encryption Barriers, TechWire, 17 June 1997.
[10] Ministry of Research and Information Technology Denmark for the European Commission Directorate-General XIII Telecommunications, Information Market and Exploitation of Research, Report of Day 1 of the European Expert Hearing on Digital Signatures and Encryption (Copenhagen, April 23, 1998), Copenhagen, Denmark, 23–24 April 1998
[11] Siemens Nixdorf, Press Release, http://www.trustedweb.com/whats—new/pressrelease.html, Hanover, Germany.
[12] Burnahm, B., The Electronic Commerce Report, Piper Jaffray Research, p. 75, August 1997.
[13] Crowell, W., Deputy Director National Security Agency, Testimony before Senate Commerce Committee, 1997.
[14] Neumann, P., et.al., The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption, Final Report of The Cryptographers' Working Group, 27 May 1997.
[15] Ibid.
[16] Ibid.
[17] Wayner, P., Administration Gets Sour Taste From Own Encryption Medicine, New York Times, 1 July 1997.
[18] Laurin, F., and Froste, C., Secret Swedish E-Mail Can Be Read by the U.S.A., Svenska Dagbladet, 18 Nov 1997.
[19] Computing, Banks Slam Snoops, 26 March 1998.
[20] Nelson, J., FBI: Commercial Spying Rises, Los Angeles Times, 12 January 1998.
[21] Ibid.

Senator FRIST. Thank you very much.
Mr. Bidzos.

STATEMENT OF D. JAMES BIDZOS, VICE CHAIR, SECURITY DYNAMICS TECHNOLOGIES, INC.

Mr. BIDZOS. Thank you, Mr. Chairman. Let me also thank you and the committee for the opportunity to be here and testify this morning. At the outset, I want to say that the PROTECT Act definitely moves us in the right direction and is a real improvement over the current administration policy, but, as I will explain in a few moments, the bill could be further improved in several important respects.

I am pleased to be here this morning and testify on behalf of Americans for Computer Privacy. ACP is a coalition of over 4,000 individuals, 40 trade associations, and over 100 companies representing financial services, manufacturing, high tech, transportation industries, as well as law enforcement, civil liberty, taxpayer, and privacy groups.

Currently I am vice chairman of Security Dynamics Technologies, but during the last 13 years I served as president and chief executive officer of RSA Data Security. RSA Data Security is the leading American company producing encryption products. It was founded in 1982 and our encryption technology is embedded in virtually every mainstream product, from things such as Microsoft Windows to Netscape's Navigator, also Microsoft's browser Internet Explorer, Intuit's Quicken, and Lotus Notes. It is very widespread. Most of it is 128 bits.

I am also the founder and chairman of a company called Verisign, which is the leader in Internet authentication and certification, and I am a director of several other security companies, including two in Japan and two in Europe. I think this has given me unique insight into the global encryption issue.

I have been deeply involved in the debate over encryption policy during this time and hope my experience can benefit the com-

mittee. I testified for the first time about 10 years ago before the House Committee on Science, Space, and Technology, and made many of the arguments that we are hearing here today.

I used to joke that encryption, the type of encryption that my company developed, was a solution in search of a problem. I do not say that any more because the problem is obvious and we have discovered it. Quite simply, it is e-commerce. E-commerce, however, is not going to reach its full potential unless it becomes secure. That would be a tremendous disappointment since electronic commerce between businesses alone is expected to reach over $300 billion per year by the year 2002. At least 60 percent of all Americans will be using the Internet and the number of worldwide online users is expected to reach 250 million by the year 2002.

Without relaxation of export controls, U.S. manufacturers remain at a competitive disadvantage and foreign consumers will purchase encryption products from foreign suppliers. Just in reaction to a comment made on the other panel, I would welcome the opportunity after my statement to go into more detail, but I think that the Administration underestimates the determination and the capabilities of the companies that we compete with overseas.

Foreign products are comparable in capabilities and quality, and do not let anyone tell you otherwise. When a foreign purchaser cannot obtain an American product, they simply purchase it from a foreign supplier. The Siemens example we heard about is a good one. There are numerous others. Indeed, foreign companies are even testifying against relaxation of U.S. export controls.

Unfortunately, not only are American companies losing the sale of an encryption item, but they are also using a sale of the program or hardware, such as an Internet server or an application browser, that incorporates the encryption capability. In fact, companies risk losing sales of entire systems because of their inability to provide necessary security features.

Over the last 13 years I have seen security move from literally out of nowhere to being No. 1, No. 2, or No. 3 on everybody's list of absolutely critical essential features in products and systems that they intend to purchase. Companies that cannot offer that essential feature are cut out of the entire business opportunity.

Thus, the only impact of the Administration's export policy is widespread deployment of foreign-designed and manufactured software and hardware.

But I think it is also essential to understand that full deployment of strong encryption is vital to America's national interest. ACP and its members are responsible citizens. We have no wish to facilitate the commission of crime or hurt national security. It is precisely because we hold these views that we believe it is in America's best interest to prevent crime and promote national security through widespread reliance on strong American encryption products both here and abroad.

We also believe that our law enforcement and intelligence agencies must be given the additional resources and technical help they need to meet the challenge of the next century. But those challenges are far greater if these agencies are forced to face a world in which the majority of information and communications systems—communications pass over systems and networks that are

foreign-designed, foreign-built, foreign-installed, and incorporate foreign encryption. That may well apply to systems here in the United States as well, based on the way things are going now.

The PROTECT Act is an improvement over current administration policy. It affirms that Americans may use and sell any type of encryption domestically and ensures that the U.S. Government may not use its full powers and capabilities to compel Americans to use or sell a certain type of encryption. The PROTECT Act also provides a broader range of export relief for American encryption products and it provides a certain timeframe for export reviews. Also, the Act provides congressional support for and sets a 5-year limit on the selection of the 128-bit Advanced Encryption Standard.

But even a good thing can be made better. The PROTECT Act should be further improved to reflect market and technological realities. The PROTECT Act does not permit individual foreign consumers to obtain strong non-recoverable encryption, making it impossible for them to securely purchase products from American companies.

Also, the Act does not provide immediate export relief for encryption sales to small businesses, one of the fastest growing worldwide business sectors. Unfortunately, the PROTECT Act limits easy exportability of mass market products with strong 128-bit encryption until NIST adopts the Advanced Encryption Standard. Exportability in the mean time is dependent on an unwieldy complex bureaucracy that will determine whether American products are generally available or compete with comparable foreign products. We believe the evidence is already overwhelming regarding these facts.

I would be happy to answer any questions about the significance of this 3-year delay in terms of how our competitors will exploit it and how that translates into Internet years and what it means for future opportunities.

In conclusion, Mr. Chairman, ACP strongly urges the committee to move forward with the PROTECT Act and to adopt amendments to permit the immediate exportability of strong encryption to a broader range of businesses and individuals abroad.

Thank you.

[The prepared statement of Mr. Bidzos follows:]

PREPARED STATEMENT OF D. JAMES BIDZOS, VICE CHAIR, SECURITY DYNAMICS TECHNOLOGIES, INC.

Congress must immediately relax export controls on software and hardware with encryption capabilities. Widespread deployment of American products with encryption capabilities will help to accelerate dramatically the growth of electronic commerce by protecting consumers' privacy and preventing electronic crime.

Without relaxation of export controls, U.S. manufacturers remain at a competitive disadvantage, and foreign consumers will purchase encryption products from foreign suppliers. Foreign products are comparable in capabilities and quality. When a foreign purchaser cannot obtain an American product they simply purchase it from a foreign supplier. Unfortunately, not only are American companies losing a sale of an encryption item, but they are also losing the sale of the program or hardware such as an Internet server or an application browser that uses the encryption capability. In fact, companies risk losing sales of entire systems because of their inability to provide necessary security features. The only impact of the Administration's export policy is widespread deployment of foreign designed and manufactured software and hardware.

The Administration took the first step towards developing a sensible long-term encryption policy by permitting exports of select products to select users, but they still have not gone far enough.

The PROTECT Act is an improvement over current Administration policy. It affirms that Americans may use and sell any type of encryption domestically, and ensures that the U.S. Government may not use its full powers and capabilities to compel Americans to use or sell a certain type of encryption. The PROTECT Act also provides a broader range of export relief for American encryption products and provides a certain timeframe for the export review process. Also, the Act provides Congressional support for, and sets a 5-year limit on the selection of, the 128-bit Advanced Encryption Standard.

The PROTECT Act should be further improved to reflect market and technological realities. The PROTECT Act does not permit individual foreign consumers to obtain strong, non-recoverable encryption, making it impossible for them to securely purchase products from American companies. Also, the Act does not provide immediate export relief for encryption sales to small businesses—one of the fastest growing worldwide business sectors.

Unfortunately, the PROTECT Act limits easy exportability of mass market products with strong 128-bit encryption until NIST adopts the Advanced Encryption Standard. This means individual consumers and small businesses will have to wait three years to obtain strong American encryption, and foreign companies will have had three more years to market their products. Exportability in the meantime is dependent on an unwieldy complex bureaucracy that will determine whether American products are generally available or compete with comparable foreign products. We believe the evidence already is overwhelming regarding these facts.

INTRODUCTION

Good Morning. My name is Jim Bidzos, and I am Vice Chair of Security Dynamics Technologies, Inc., a Massachusetts-based security firm that is also the parent company of RSA Data Security, located in San Mateo, California. For over 13 years, until earlier this year, I was the President and CEO of RSA Data Security, the world's leading encryption company.

RSA's technology is embedded in both Netscape and Microsoft browsers, and in over 500 other products, all used by hundreds of millions of people around the world to secure internet transactions and digital data of many types. Over many years, I have personally negotiated hundreds of licenses to RSA encryption technology, including licenses with companies such as IBM, Microsoft, ATT, Netscape, Oracle, and Motorola. These negotiations almost always involve discussions about encryption needs, end-user requirements, and export policy. I have thus gained unique insights into the needs and concerns of both industry and users with respect to encryption.

I am also founder and chairman of Verisign, Inc., the leader in Internet authentication. Verisign is the world's largest Internet security products and services company as measured by both customers and market capitalization.

I am a member of the board of directors of several other security companies. One specializes in virtual private networks. Another is a manufacturer of security tokens. Another offers cryptographically secure digital time stamping services. I am also a director of a UK-based encryption hardware company, a Dublin-based secure electronic payments company, and two Japanese security companies.

I have been deeply involved in the debate over encryption, from many aspects, including US policy on the export of this technology. Over the last 13 years, I have testified many times before both the House and Senate on encryption policy, and I have participated in numerous US and international standards activities.

I believe that my long and unique history in the encryption area allows me to offer testimony today that may help the committee better understand industry's concerns over US encryption policy.

On behalf of Americans for Computer Privacy ("ACP"), thank you for the opportunity to testify on S.798, the PROTECT Act, sponsored by Chairman McCain and cosponsored by four other committee members Senators Bums, Wyden, Abraham, and Kerry.

ACP is a coalition of over 3,500 individuals, 40 trade associations and over 100 companies representing financial services, manufacturing, high-tech, and transportation industries as well as law enforcement, civil-liberty, taxpayer and privacy groups. ACP supports policies that allow American citizens to continue using strong encryption without government intrusion, and advocates the lifting of export restrictions of U.S. made encryption products.

But we really are here today to speak on behalf of the tens of millions of users of American software and hardware products. The American software and hardware

industries have 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 interact securely worldwide. American companies have innovative products which can meet this demand and compete internationally. But there is one thing in our way—the continued application of overbroad, unilateral, export controls by the U.S. Government.

At the outset, I want to say that the PROTECT Act definitely moves us in the right direction and is a significant improvement over the Administration's current policy—but it *could* be further improved in several important respects (along the lines of the SAFE Act).

ACP recognizes a legitimate governmental need to obtain access to information and communications when authorized by proper legal authority. ACP and its members are responsible citizens. We have no wish to facilitate the commission of crime or the spread of terrorism. Similarly, we are committed to strengthening the nation's infrastructure and promoting national security, enhancing the privacy of American citizens and ensuring the security of electronic commerce.

But we believe that the best way of meeting all these objectives is promote the widespread use of encryption!

Ultimately, any truly successful, sensible encryption policy that has America's best interests at heart must be based on technological and market realities, and should not create winners and losers in the encryption marketplace on a sector-by-sector basis. It would recognize that:

- The worldwide encryption standard is 128-bit encryption;
- Mass market software and hardware is inherently uncontrollable; and
- It is in America's national and economic security interests to have American designed and manufactured encryption products deployed worldwide.

We believe it is preferable for Congress to put encryption policy on a statutory basis rather than continuing to leave it up to inconsistent Administration regulations—sending a strong message around the world that encryption is important for protecting the privacy of citizens, for promoting e-commerce, preventing crime and protecting our critical infrastructures and national defense.

THE AMERICAN COMPUTER SOFTWARE AND HARDWARE INDUSTRIES—AN AMERICAN SUCCESS STORY

The computer software and hardware industries are American success stories, but they are being threatened. America's software and hardware industries are important contributors to U.S. economic security. Information technology industries now are directly responsible for over one-third of real growth of the U.S. economy, and both the computer and software industries are continuing to grow. From 1990 through 1996, the software industry grew at a rate of 12.5%, nearly 2.5 times faster than the overall U.S. economy.

More than 7 million people work in IT industries. In 1996, the software industry provided a total of over 619,000 direct jobs and $7.2 billion in tax revenues for the U.S. economy. The software industry is expected to create an average of 45,700 new jobs each year through 2005. If piracy were to be eliminated in the United States, the number of new software jobs created would double to an average of 93,000 a year.

Moreover, the computer software industry has achieved tremendous success in the international marketplace with global sales of packaged (i.e., non-custom) software reaching over $118.4 billion in 1996, and rising to $135.4 billion in 1997. American produced software accounts for 70% of the world market, with exports of U.S. programs constituting half of the industry's output.

The incredible growth of the industry and its exporting success benefits America through the creation of jobs here in the United States. Many of these jobs are in highly skilled and highly paid areas such as research and development, manufacturing and production, sales, marketing, professional services, custom programming, technical support and administrative functions. In the U.S. software industry, workers enjoy more than twice the average level of wages across the entire economy—$57,319 versus $27,845 per person.

All of these revenues and jobs are dependent upon American software and hardware producers remaining the market leaders around the world, especially as the major growth markets continue to be outside the United States. Strong export controls on products with encryption capabilities are crippling the ability of these companies to compete with foreign providers and are only ensuring that foreign products are securing worldwide critical infrastructures, not American products.

SECURE NETWORKS AND CONFIDENTIAL INFORMATION IN THE INTERNET AGE ARE THE KEY TO PRIVACY AND COMMERCE

American individuals and companies are rapidly becoming networked together through private local area networks (LANs), wide area networks (WANs) and public networks such as the Internet. Combined, these private and public networks are the economic engine driving electronic commerce, transactions and communications. This engine is sputtering and threatens to stall.

Traffic on the Internet doubles every 100 days. Predictions of business-to-business Internet commerce for the year 2000 range from $66 billion to $171 billion, and by 2002, electronic commerce between businesses is expected to reach $300 billion. During 1997, one leading manufacturer of computer software and hardware sold $3 million per day online for a total of $ 1.1 billion for the year.

More and more individual consumers also are going on line arid spending. Five years from today, we anticipate nearly 60 percent of all Americans to be using the Internet. More than 10 million people in North America alone have already purchased something over the Internet, and at least 40 million have obtained product and price information on the Internet only to make the final purchase off-line. Altogether last year, consumers spent nearly $8 billion online. Nearly 1.5 million Americans join the online population every month, and the number of worldwide online users is expected to reach 248 million by 2002.

The incredible participation by American consumers in the Internet phenomenon clearly demonstrates that the need for strong encryption is no longer merely the purview of our national security agencies concerned about securing data and communications from interception by foreign governments. Today, every American even merely dabbling on the Internet requires access to strong encryption. Imagine the boost in volume of e-commerce if all of these consumers had enough confidence in the security of the Internet to purchase on-line. Yet in 1996 the Computer Security Institute/FBI Computer Crime Survey indicated that our worldwide corporations will be increasingly under siege: over half from within the corporation, and nearly half from outside of their internal networks.

Network users *must* have confidence that their communications and data—whether personal letters, financial transactions or sensitive business information—are secure and private. Electronic commerce is transforming the marketplace—eliminating geographic boundaries and opening the world to buyers and sellers. Companies, governments and individuals now realize that they can no longer protect data and communications from others by relying on limiting physical access to computers and maintaining stand-alone centralized mainframes. Instead, users expect to be able to pick up their e-mail or modify a document from any computer anywhere in the world simply by using their Internet browsers. Thus, consumers worldwide are demanding to be able to protect their electronic information and interact securely worldwide, and access to products with strong encryption capabilities has become critical to providing them with confidence that they will have this ability.

UNILATERAL U.S. EXPORT CONTROLS HARM AMERICAN INTERESTS

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 products that offer strong encryption capabilities.

American companies are forced to limit the strength of their encryption to the 56-bit key length level set late in 1998. The recently announced regulations will also permit companies to export stronger encryption on a sector-by-sector, user-by-user basis. However, this policy ignores the fact that:

• The minimum strength now required by new Internet applications is 128-bit encryption;

• American companies cannot export encryption products to a vast majority of non-U.S. commercial entities. Foreign manufacturers provide 128-bit encryption alternatives and add-ons—filling the market void created by U.S. export controls;

• Providing sector-by-sector relief is unworkable for mass market products and does not reflect commercial realities for sales of custom products;

• 56-bit encryption has been demonstrated to be vulnerable to commercial let alone governmental attack. (In the beginning of this year at the RSA Encryption Conference, a 56-bit DES encoded message was broken by private companies and individuals working together in 22 hours and 15 minutes—imagine what a hostile government with serious resources could do); and

• New developments in technology are introduced everyday that speed up decryption time. Adi Shamir, the Israeli computer scientist who is the "S" in RSA, recently announced "Twinkle", which is a proposed method for quickly unscrambling

computer-generated codes that have until now been considered secure, at the International Association for Cryptographic Research's latest meeting in Prague.

THE WASSENAAR ARRANGEMENT IS NOT A MULTILATERAL AGREEMENT TO CONTROL ENCRYPTION

I want to take one minute to discuss the Wassenaar Arrangement at this point. Please do not be fooled by any claims from the Administration that the Wassenaar Arrangement is the multilateral agreement on encryption that they have been touting was just around the corner for the past several years.

The Wassenaar Arrangement replaced the old COCOM regime with a non-binding agreement among 30 countries to report on their sensitive exports. The December 1998 Wassenaar Arrangement agreement actually *decontrolled* encryption products. Many countries, such as Israel and South Africa, who export strong encryption are not signatories to the Arrangement. The Wassenaar Arrangement eliminates controls of any sort on 56-bit encryption and permits exports of up to 64-bit encryption in mass-market software and hardware. It also removed any reporting requirements—the sole official means for actually monitoring what countries are doing. Although the Arrangement left open the possibility that countries might individually control 128-bit encryption, we are skeptical that they will do so. There is no penalty for failing to control 128-bit encryption, and most countries are actually moving towards *encouraging* the use of stronger encryption. Finally, a country could technically comply with the Arrangement, while still permitting easy exports of strong encryption.

Ironically, the U.S. government is a good example of the lack of effect of the Wassenaar Arrangement. In its new encryption regulations, the Administration is still controlling encryption products with greater than 56, not 64, bit keys, and they have imposed reporting requirements on mass market products even if they are using 64-bit encryption.

Recently, on June 2, 1999, the German government established a new encryption policy seeking to improve protection of German users of global information networks and clarifying that any encryption product may be developed, produced marketed and used without restrictions in Germany. The German government declared its intention to simplify their export review process and to strengthen the performance and ability of German manufacturers to compete internationally. The German government will monitor abuses of encryption for illegal purposes and attempt to further improve the technical capabilities of German law enforcement and security agencies to handle advances in encryption technology.

Even France, traditionally the country which placed the greatest restrictions on its own citizens by limiting them to the easily broken 40-bit level of encryption, has recognized that technology has progressed. Near the end of 1998, France relaxed controls on the domestic use of encryption and is now permitting, and in fact encouraging, the use of 128-bit encryption by its citizens.

WITHOUT EXPORT RELIEF, FOREIGN CONSUMERS WILL PURCHASE THEIR PRODUCTS FROM FOREIGN SUPPLIERS, KEEPING U.S. MANUFACTURERS AT A COMPETITIVE DISADVANTAGE

Export controls also have made American companies less competitive and opened the door for foreign software and hardware developers to gain significant market share—decreasing our national and economic security.

As a result of U.S. unilateral export controls, encryption expertise is being developed off-shore by foreign manufacturers who now provide hundreds of encryption alternatives and add-ons. The Administration's export controls are in no way preventing foreigners, let alone those with criminal intent, from obtaining access to encryption products. In fact, foreign software and hardware manufacturers have seized the opportunity to create sophisticated encryption products and to capture sales.

As long ago as 1995, the General Accounting Office confirmed that sophisticated a encryption software is widely available to foreign users on foreign Internet sites. In 1996, a Department of Commerce study again confirmed the widespread availability of foreign manufactured encryption programs and products. Professor Hoffman today releases the results of his latest survey which shows the continuing growth in foreign encryption products in the face of U.S. export controls.

If an encryption product is combined with other applications such as Internet browsers and application servers, U.S. companies generally will lose both sales. In fact, companies risk losing sales of entire systems because of inability to provide necessary security features. This permits foreign manufacturers to gain entry into

companies as well as gain credibility—providing the foreign manufacturers with further opportunity to take away future sales in the same and other product lines.

U.S. ENCRYPTION EXPORT CONTROLS HURT AMERICAN COMPANIES WITHOUT HELPING LAW ENFORCEMENT OR NATIONAL SECURITY

U.S. export controls have had the effect of creating an encryption expertise outside the United States that is gathering momentum. Unfortunately, every time research and development of an encryption technique or product moves off-shore, U.S. law enforcement and national security agencies lose. We believe that continuing down this path will be ultimately more harmful to our national security and law enforcement efforts as American companies will no longer be the world leaders in creating and developing encryption products.

In fact, as long ago as 1996, the NRC Committee concluded that as demand for products with encryption capabilities grows worldwide, foreign competition could emerge at levels significant enough to damage the present U.S. world leadership in information technology products. The Committee felt it was important to ensure the continued economic growth and leadership of key U.S. industries and businesses in an increasingly global economy, including American computer, software and communications companies. Correspondingly, the Committee called for an immediate and easy exportability of products meeting general commercial requirements—which is currently 128-bit level encryption!

To summarize:

• Foreign competitors not subject to outdated U.S. export controls are ready to take sales and customers from U.S. companies today.

• Complex and cumbersome U.S. export controls make American companies less competitive. They significantly increase the costs of developing, marketing and selling products with encryption capabilities, delay the introduction of new products or features, and encourage foreign customers to purchase from foreign suppliers due to the uncertainty and delay in obtaining a comparable American product.

• Current export controls do not keep strong encryption out of the hands of foreign customers; they just keep U.S. products out of their hands.

• In the future, if export controls on encryption are not relaxed, both American and foreign infrastructures will be secured by foreign encryption products, creating a significant problem for American law enforcement and national security agencies.

American companies *do* have exciting and innovative products that can meet the demand for 128-bit encryption and compete internationally. But unless the current unilateral U.S; export restrictions are changed to allow the use of strong encryption, American individuals and businesses will not be active participants in this new networked world of commerce—let alone continue to be the leaders in its development. Furthermore, American companies will no longer be providing the world, and its critical infrastructures, with the answers to their security problems. Instead foreign companies will. It is unclear how U.S. national security or law enforcement will be aided or how our critical infrastructures will be secure when foreign encryption products dominate the world market.

THE BERNSTEIN CASE

The absurdity of the existing export control regime is further highlighted by the recent decision of the 9th Circuit Court of Appeals in *Bernstein* v. *DOJ*. In that case, the court held that the existing restrictions on the export of source code, the language in which programmers communicate their ideas to one another, are an unconstitutional prior restraint on first amendment rights of free speech. So now we have a situation where it is permissible to export jobs (because one can export source code to teach foreign programmers), but not American products (because one cannot embody that source code in a product)!

More generally, Judge Fletcher's opinion raises some very valid, more general questions and points out how important encryption is to the mainstream life of Americans rather than merely to obscure technologists. Judge Fletcher states:

> In this increasingly electronic age, we are all required in our everyday lives to rely on modern technology to communicate with one another. This reliance on electronic communication, however, has brought with it a dramatic diminution in our ability to communicate privately. Cellular phones are subject to monitoring, email is easily intercepted, and transactions over the internet are often less than secure. Something as commonplace as furnishing our credit card number, social security number, or bank account number puts each of us at risk. Moreover, when we employ electronic methods of communication, we often leave electronic "fingerprints" behind, fingerprints that can be traced back to us. Whether we are surveilled by our government, by criminals, or by our neigh-

bors, it is fair to say that never has our ability to shield our affairs from prying eyes been at such a low ebb. The availability and use of secure encryption may offer an opportunity to reclaim some portion of the privacy we have lost. Government efforts to control encryption thus may well implicate not only the First Amendment rights of cryptographers intent on pushing the boundaries of their science, but also the constitutional rights of each of us as potential recipients of encryption's bounty. Viewed from this perspective, the government's efforts to retard progress in cryptography may implicate the Fourth Amendment, as well as the right to speak anonymously, . . ., the right against compelled speech, . . ., and the right to informational privacy. While we leave for another day the resolution of these difficult issues, it is important to point out that Bernstein's is a suit not merely concerning a small group of scientists laboring in an esoteric field, but also touches on the public interest broadly defined.

THE ADMINISTRATION TOOK A SMALL FIRST STEP TOWARDS DEVELOPING A SENSIBLE LONG-TERM ENCRYPTION POLICY, BUT THEY STILL HAVE NOT GONE FAR ENOUGH

Progress was made last year in the new Administration policy announced by the Vice President in September and contained in the interim final regulations of December 31, 1998.

ACP welcomed the Administration's efforts to relax export controls on select products used by select users. We especially appreciated the Administration's apparent abandonment of its key escrow policy that would have required all encryption exports (except for 40-bit and less encryption) to be capable of providing third parties with immediate access to the plaintext of stored data or communications without the knowledge of the user. Foreign companies and consumers simply would not purchase such products as a multitude of foreign products without key escrow are readily available.

However, the Administration's actions are merely a first step. U.S. export controls still ignore the realities of mass-market software and hardware distribution. Mass-market software publishers and hardware manufacturers sell products through multiple distribution channels such as OEMs (ie., hardware manufacturers that preload software onto computers), value-added resellers, retail stores and the emerging channel of on-line distribution. Thus, mass market products are available to the general public from a variety of sources. (It also is why continued reporting requirements about end-uses and end-users make no sense.)

The mass-market distribution model presupposes that software publishers and hardware manufacturers 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. As mass market products are uncontrollable, ACP believes U.S. companies should be able to export the current market standard of 128-bit encryption. Unfortunately, the Administration has only proposed permitting easy exports of 56-bit encryption even if foreign products exist in the marketplace.

ACP also believes that encryption hardware and software should be treated identically. However, contrary to the Administration's original announcement regarding export relief which included export relief for hardware, the new regulations still do not permit 56-bit encryption chips, integrated circuits, toolkits and executable or linkable modules to be easily exported except to subsidiaries of U.S. companies or otherwise relax export controls on stronger mass market hardware.

In addition, ACP believes that the new regulations are so complex and contain unrealistic requirements that they undermine many of the benefits of the Administration's export relief for stronger encryption, especially for mass market hardware and software. U.S. companies are now required to meet a number of new, unilateral reporting requirements. For example, exporters now are required to report the name and address of end-users, a virtual impossibility for mass-market exporters because registration of end-users is customarily voluntary. A system to obtain the names and addresses of each of the millions of potential health care end-users, for example, would cost more than the profits yielded from many products.

ACP also is disappointed that the Administration's regulations do not clearly provide online merchants with the level of export control relief originally envisioned as they do not permit ISPs to provide "services" as a permissible end-use. This could chill the use by ISPs located abroad of U.S.-origin encryption products for billing, payment, and delivery purposes, despite the widespread foreign availability of such products.

THE PROTECT ACT IS AN IMPROVEMENT OVER CURRENT ADMINISTRATION POLICY

The PROTECT Act Establishes The Correct Domestic Encryption Policy

The PROTECT Act affirms that Americans may use and sell any type of encryption domestically. Even more importantly, the PROTECT Act ensures that the U.S. Government may not use its full powers and capabilities to compel, directly or indirectly, Americans to use or sell a certain type of encryption. This will prevent the U.S. Government from attempting to achieve domestic controls on encryption through regulations or "incentives".

For example, the Act prohibits the U.S. Government from linking the ability to electronically sign a document to a requirement that the consumer use a particular encryption methodology for ensuring confidentiality. Thus, the U.S. Government cannot require Americans to use a certain type of encryption (such as key escrow) to engage in electronic commerce.

Also, the PROTECT Act specifically restricts the government from requiring any American to use a particular encryption product or methodology to communicate with or transact business with the government. The U.S. Government may only specify technologies for its own internal uses.

The PROTECT Act Provides Additional Export Relief For Encryption Products

The PROTECT Act provides a broader range of export relief for American encryption products than the Administration. We are pleased that the PROTECT Act provides immediate export relief after a one-time review by the government for:

- All encryption products using key lengths of 64-bits or less rather than the less secure 56-bit key lengths proposed by the Administration;
- All recoverable encryption products regardless of key length, including telecommunications related products; and
- All encryption products using key lengths greater than 64-bits to certain legitimate and responsible commercial users, including publicly traded firms, firms subject to government regulation, U.S. companies' foreign subsidiaries, affiliates and strategic partners, on-line merchants who use encryption products to support electronic commerce, and foreign governments who are members of NATO, OECD and ASEAN.

We are also pleased that the PROTECT Act recognizes the need for a quicker and more certain timeframe for the export review process. Businesses simply cannot live with the U.S. Government taking between 3 to 6 months to determine whether a product is exportable when many Internet products have 90 day product cycles and most businesses do not want to wait through one or two business quarters to update their computer systems.

The PROTECT Act Begins To Recognize Mass Market Product Realities

We also are encouraged that the PROTECT Act recognizes the difficulties in complying with reporting requirements for mass market encryption products and eliminates such reporting requirements. It is virtually impossible for mass-market exporters to report the name and address of each end-user. Millions of these products are sold through multi-level distribution channels (e.g., VAR's and chain stores). Moreover, as registration of mass market products is customarily voluntary. This is a vast improvement over the Administration's proposed regulations which effectively require companies to develop a system to obtain the names and addresses for each health and medical end-user of stronger encryption products and all foreign online merchants.

The PROTECT Act also provides Congressional support for, and sets a 5-year limit on the selection of, the 128-bit Advanced Encryption Standard which is being developed under the auspices of the National Institute of Standards and Technology. The 2002 deadline will provide impetus for NIST to finish developing the standard in a timely manner while providing NIST with sufficient time to study the final standard's security features. This is an important process that will result in a new standard for government's sensitive, but unclassified, information and most likely will serve as the new worldwide standard for strong encryption simiiar to the Data Encryption Standard when it was introduced in the 1970's. Once the algorithm is selected, the PROTECT Act removes all export controls on encryption products using the 128-bit standard or its equivalent strength.

THE PROTECT ACT SHOULD BE FURTHER IMPROVED TO REFLECT MARKET AND TECHNOLOGICAL REALITIES

The PROTECT Act Does Not Provide Immediate Export Relief For Individual Consumers

The PROTECT Act does not go far enough to protect the millions and millions of consumers that are now engaging in electronic commerce. Foreign consumers still will not be able to obtain an American Internet browser with strong, non-recoverable encryption, making it impossible for them to securely purchase products from American companies. Also, an everyday foreign consumer who wants to protect an on-line diary, copies of health care records or a business proposal, may not easily obtain strong encryption to do so from American sources if any portion of the encryption used by the product is non-recoverable. Under the bill, all these individuals must wait until 2002.

The PROTECT Act Does Not Provide Immediate Export Relief For Small Businesses

We believe the PROTECT Act provides greater export relief for larger corporate customers. However, until 2002, small and privately-owned businesses face significant difficulty in easily obtaining U.S. encryption under any of the License Exceptions established by the PROTECT Act. So, for example, if two doctors in private practice together in Brazil or a restaurant owner in France or a small shopping market in Germany wants to purchase non-recoverable encryption, these small businesses probably would purchase a comparable foreign product as an American company could not easily export it to them.

Unfortunately, as companies install the security "plumbing" into their individual computers and company networks, it becomes increasingly difficult for American companies to replace the foreign software and hardware that already has been installed. Because the small business sector is, and most likely will continue to be, the fastest growing business sector, this puts American companies at a distinct disadvantage in selling encryption products at a later date.

The PROTECT Act's Export Relief For Mass Market Products And For Products Which Face Competition From Comparable Foreign Products Is Too Complicated And Creates An Unwieldy Bureaucracy

The PROTECT Act does recognize that mass market and publicly available encryption products, and encryption products for which comparable foreign products are available, should be treated differently under the U.S. export regime. The bill acknowledges the futility of trying to control a product that can be bought off of the Internet or easily purchased from commercial vendors such as CompUSA or from Circuit City by any individual in America regardless of nationality, or a comparable product can be easily purchased from similar stores in a foreign country. "Bad guys" certainly will have no problems obtaining the encryption products, and no concerns about "exporting" the products via telephone lines or the Internet or smuggled out on personally pressed CDs. The only impact of the export controls will be to stop American companies from selling American products to legitimate users.

Unfortunately, the PROTECT Act establishes a complicated private/public board structure for deciding after-the-fact whether or not a product is a mass market product or whether comparable foreign products are available. The Secretary of Commerce has thirty days to approve or disapprove the Board determination, subject to judicial review, and the President may override any determination. Unfortunately, there is no guarantee of any consistency in the Board's decisions. Thus, while the Board procedure is an improvement, and the opportunity for judicial review provides a mechanism to ensure that exports are not denied in an arbitrary and capricious manner, it is not a predictable, clear process giving American companies certainty as to whether they can export their products. Such predictability is necessary so that American companies can have confidence designing and building security features into their products.

The PROTECT Act should, but does not, afford complete and immediate export relief for mass market encryption without any complicated oversight. The Act also does not recognize that if a comparable foreign product is available, any delay in exports provides a significant advantage to the foreign product.

The PROTECT Act's Relief For 128-Bit AES Products Is Too Little, Too Late

I want to make one final comment regarding the general exportability of mass market products. We support NIST's efforts to establish a new 128-bit Advanced Encryption Standard; however, under the bill, it will not be finalized until 2002. Because the PROTECT Act limits easy exportability of mass market products until the AES is adopted, general distribution of these products will have to wait almost three years. Considering the current speed of technological change, where Internet prod-

ucts are now on three-month product cycle times, and the fact that 128-bit comparable foreign encryption is currently available, this is an eternity in Internet time. Law enforcement and national security interests have known for a long time that ubiquitous use of strong encryption by consumers worldwide is just around the corner. They cannot hope to continue to delay the world from using strong encryption according to their timeframe.

THE TIME FOR ACTION IS NOW

To keep American vendors on a level international playing field and American computer users adequately protected, U.S. export controls must be immediately updated to reflect technological and international market realities.

Thank you.

Senator FRIST. Thank you, Mr. Bidzos.

Dr. Hoffman.

STATEMENT OF LANCE J. HOFFMAN, PH.D., PROFESSOR, DEPARTMENT OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE, AND DIRECTOR OF THE SCHOOL OF ENGINEERING AND APPLIED SCIENCE, CYBERSPACE POLICY INSTITUTE, THE GEORGE WASHINGTON UNIVERSITY

Dr. HOFFMAN. Thank you, Mr. Chairman. I appreciate the opportunity to be here this morning. I will give an abridgment of my written statement which has been previously furnished to this committee.

My name is Lance Hoffman. I am a professor in the Department of Electrical Engineering and Computer Science at The George Washington University here in Washington, DC. I am also director of the School of Engineering's Cyberspace Policy Institute and the author or editor of five books and numerous articles on computer security and privacy. My most recent book is a compendium of papers on the encryption policy problem entitled "Building in Big Brother."

Our Institute recently produced a report which we are releasing today, which I think you have been furnished, entitled "Growing Development of Foreign Encryption Products in the Face of U.S. Export Regulations." This report is also available from the Institute and will be available later on this afternoon on our web site, where detailed tables and charts supporting the testimony I am giving are available.

We did this work in cooperation with NAI Labs, the Security Research Division of Network Associates in Glenwood, MD. The project manager for NAI Labs, Dave Balenson, is with me today. We were assisted in this project by three students.

In our work, we found that the development of cryptographic products outside the United States is not only continuing, but is expanding to additional countries. With the rapid growth of the Internet, communications-related cryptography especially has been experiencing high growth.

We identified 805 hardware and/or software products which incorporate cryptography. These were manufactured in 35 countries outside the United States. Attachment 1 to the written testimony provides the details on the countries and products.

These 805 foreign cryptographic products represent a 149-product increase, or 22 percent, over the most recent previous survey in December 1997. At least 167 of these use strong encryption, the

kind that one cannot export from the United States without applying for and receiving export license approval.

Cryptography product manufacturers have appeared in six new countries since December 1997: Estonia, Iceland, Isle of Man, Romania, South Korea, and Turkey. In established markets, there have been some large increases in the number of products offered. For example, the United Kingdom jumped by 20 products and Germany jumped by 28 products, going from 76 to 104.

Mr. Chairman, in 70 countries outside the United States, foreign companies are manufacturing or distributing cryptographic products. We found 512 of these companies. On average, the quality of foreign and U.S. products is comparable and there are a number of very good foreign encryption products that are quite competitive in strength, standards compliance, and functionality.

A significant number of foreign competitors to U.S. manufacturers are developing products with strong encryption and have as customers a number of large foreign or multinational corporations. Our report gives more detail on some of these companies and their offerings.

We also found some examples of advertising used by non-U.S. companies that generally attempted to create the perception that purchasing American products may involve significant red tape and the encryption may not be strong due to export controls. Cited earlier this morning was material from Cybernetica's web site in Estonia, and that is also in the written testimony.

Mr. Chairman, companies want to sell encryption products that meet certain accepted worldwide standards. To give you just two examples, in the case of IPsec, the Internet Protocol Security Standard, there are implementations from at least nine companies in five foreign countries. One of these is a joint effort of several Japanese companies, including Fujitsu, Hitachi, Toshiba, and NEC.

Two years ago NIST solicited algorithms for the Advanced Encryption Standard to replace the Data Encryption Standard, DES, as the U.S. Government standard. The majority of the 15 candidate algorithms submitted came from foreign countries. So it is very possible that the next U.S. Government encryption standard will have been designed outside the United States.

Finally, Mr. Chairman, our empirical product data could be combined with economic measures and economic theories to better explain why we are seeing this observed growth in the cryptography marketplace and to examine the effects of Internet growth, electronic commerce development, and regulatory actions on the market over time. With this knowledge, we would be able to more easily adjust our national laws for a global economy.

Thank you.

[The prepared statement of Dr. Hoffman follows:]

PREPARED STATEMENT OF LANCE J. HOFFMAN, PH.D. PROFESSOR, DEPARTMENT OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE, AND DIRECTOR OF THE SCHOOL OF ENGINEERING AND APPLIED SCIENCE, CYBERSPACE POLICY INSTITUTE, THE GEORGE WASHINGTON UNIVERSITY

My name is Lance J. Hoffman. I am a professor in the Department of Electrical Engineering and Computer Science at The George Washington University in Washington, D.C. I also am Director of the School of Engineering's Cyberspace Policy Institute and the author or editor of five books and numerous articles on computer security and privacy. My most recent book is a compendium of papers on the

encryption policy problem entitled Building in Big Brother (Springer-Verlag, New York, 1995).

Currently, I am the principal investigator for a project entitled "Cryptography Products and Market Survey". As part of that project, we have recently produced a report entitled "Growing Development of Foreign Encryption Products in the Face of U.S. Export Regulations". I am leaving you copies of that report, which is also available from the Institute or on our Web site at http://www.seas.gwu.edu/seas/institutes/cpi/library/papers.html, where detailed tables and charts supporting this testimony are also available. We did this work in cooperation with NAI Labs, the Security Research Division of Network Associates, Inc., Glenwood, Md. The project manager for NAI Labs, Mr. David Balenson, is with me today. We were assisted in this project by three students.

In the project, we surveyed encryption products developed outside the United States and found that the development of cryptographic products outside the United States is not only continuing but is expanding to additional countries; with rapid growth of the Internet, communications-related cryptography especially is experiencing high growth.

As of June 8, 1999, we identified 805 hardware and/or software products incorporating cryptography manufactured in 35 countries outside the United States. As shown in Attachment 1, the greatest number of foreign cryptographic products are manufactured in the United Kingdom, followed by Germany, Canada, Australia, Switzerland, Sweden, the Netherlands, and Israel in that order. Other countries accounted for slightly more than a quarter of the world's total of encryption products.

These 805 foreign cryptographic products represent a 149-product increase (22%) over the most recent previous survey in December 1997. At least 167 of them use strong encryption, the kind that one cannot export from the United States without applying for and receiving export license approval. The algorithms used in these are Triple DES, IDEA, BLOWFISH, CAST–128, or RC5.

Cryptography product manufacturers have appeared in six new countries since December 1997: Estonia, Iceland, Isle of Man, Romania, South Korea, and Turkey. There has also been a large increase in the number of products produced by certain countries. The United Kingdom jumped by 20 products from 119 to 139, and Germany jumped from 76 products to 104. Also notable was Japan's increase, from 6 products to 18, and Mexico's, from a single product to six.

There are now 512 foreign companies that either manufacture or distribute foreign cryptographic products in 70 countries outside the United States. Attachment 2 lists these countries.

On average, the quality of foreign and U.S. products is comparable. We have encountered poor products both within and outside the U.S., and we have encountered good products both within and outside the U.S. There are a number of very good foreign encryption products that are quite competitive in strength, standards compliance, and functionality.

A significant number of foreign competitors to U.S. manufacturers of software and hardware with encryption capabilities are developing products with strong encryption, and have as customers a number of large foreign or multinational corporations. The report gives thumbnail sketches of some of these companies and their offerings.

We found some example of advertising used by non-U.S. companies that generally attempted to create the perception that purchasing American products may involve significant red tape and the encryption may not be strong due to export controls. As an example, we show in Attachment 3 material from Cybernetica's Web site in Estonia. We give several other examples of similar advertising in the report.

Companies want to sell encryption products that meet certain accepted worldwide standards. Encryption experts from all over the world have contributed to two important international standards efforts, IPsec and the Advanced Encryption Standard. In the case of IPsec, there are currently implementations (complete or in the works) from at least nine companies in five foreign countries. One effort, the KAME Project, is a joint effort of several Japanese companies (Fujitsu, Hitachi, IIJ Research Laboratory, NEC, Toshiba, and Yokogawa).

In 1997, the National Institute of Standards and Technology (NIST) solicited algorithms for the Advanced Encryption Standard (AES) to replace the Data Encryption Standard (DES) as a U.S. government encryption standard. Individuals and companies from eleven different foreign countries proposed 10 out of the 15 candidate algorithms submitted to NIST. So it is very possible that the next U.S. government encryption standard will have been designed outside the United States. Details on who submitted what algorithm are given in Attachment 4.

Finally, our empirical product data could be combined with economic measures and economic theories to better explain why we are seeing the observed growth in

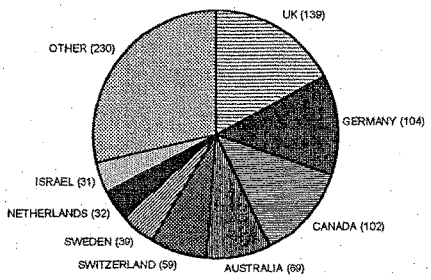
the cryptography marketplace, and to examine the effects of Internet growth, e-commerce development, and regulatory actions on the international cryptographic market over time, thus getting better insights into the implications of various policy options. We should be able to combine previous work with studies already available on the information technology sector and the data in our study to better understand the changes we are seeing in the global marketplace, and thus be able to more easily adjust national laws for a global economy.

Attachment 1. Foreign Cryptographic Products by Country

Foreign Cryptographic Survey Results (as of May 1999)

The updated survey identified a total of 805 foreign cryptographic products from 35 countries:

Argentina	Australia	Austria
Belgium	Canada	Czech Republic
Denmark	Estonia	Finland
France	Germany	Greece
Hong Kong	Iceland	India
Iran	Ireland	Isle Of Man
Israel	Italy	Japan
Mexico	Netherlands	New Zealand
Norway	Poland	Romania
Russia	South Africa	South Korea
Spain	Sweden	Switzerland
Turkey	UK	



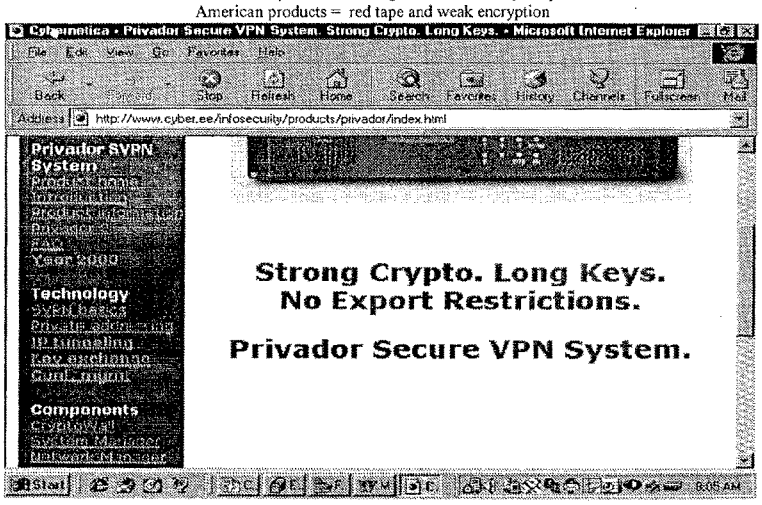
At least 167 of these foreign cryptographic products implement "strong" cryptographic algorithms, including Triple DES, IDEA, BLOWFISH, RC5, or CAST.

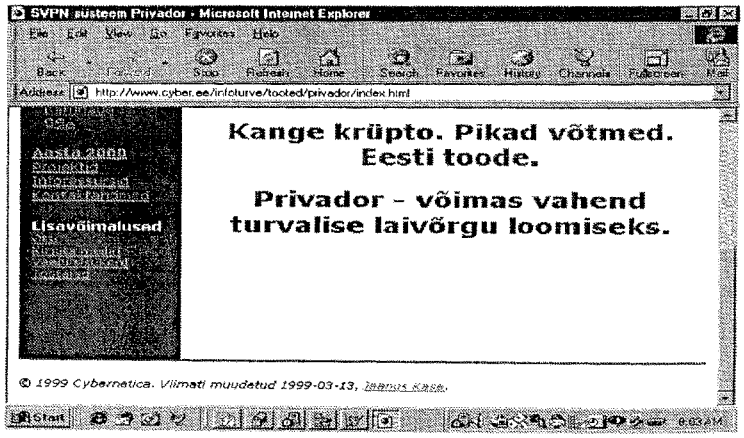
We identified 512 foreign cryptography companies (including distributors as well as manufacturers) in 70 countries.

Attachment 2. Foreign countries in which cryptography is manufactured or distributed

Argentina
Australia
Austria
Bahrain
Baltic Republics
Bangladesh
Belgium
Brazil
Brunei
Canada
Chile
Colombia
Cyprus
Czech Republic
Denmark
Estonia
Finland
France
Germany
Ghana
Greece
Hong Kong
Iceland
India
Indonesia
Iran
Ireland
Isle of Man
Israel
Italy
Ivory Coast
Japan
Kenya
Kuwait
Luxembourg
Madagascar
Malaysia
Malta
Mauritius
Mexico
Nepal
Netherlands
New Zealand
Nigeria
Norway
Oman
Philippines
Poland
Portugal
Qatar
Reunion
Romania
Russia
Saudi Arabia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Turkey
United Arab Emirates
United Kingdom
Venezuela
West Indies
Yugoslavia
Zimbabwe

Attachment 3. Example of advertising used to create a perception that American products = red tape and weak encryption





Attachment 4. Proposed Candidates for Advanced Encryption Standard

Country	Candidate Algorithm	Submittor(s)
Australia	LOKI97	Lawrie Brown, Josef Pieprzyk, Jennifer Seberry
Belgium	RIJNDAEL	Joan Daemen, Vincent Rijmen
Canada	CAST-256	Entrust Technologies, Inc.
	DEAL	Outerbridge, Knudsen
Costa Rica	FROG	TecApro Internacional S.A.
France	DFC	Centre National pour la Recherche Scientifique (CNRS)
German	MAGENTA	Deutsche Telekom AG
Japan	E2	Nippon Telegraph and Telephone Corporation (NTT)
Korea	CRYPTON	Future Systems, Inc.
USA	HPC	Rich Schroeppel
	MARS	IBM
	RC6	RSA Laboratories
	SAFER+	Cylink Corporation
	TWOFISH	Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson
UK/Israel/Norway	SERPENT	Ross Anderson, Eli Biham, Lars Knudsen

Smid, M., and M. Dworkin, Special Report on the First AES Conference, presented at Crypto '98 Conference, August 1998, http://csrc.nist.gov/encryption/aes/round1/crypto98.pdf.

GROWING DEVELOPMENT OF FOREIGN ENCRYPTION PRODUCTS IN THE FACE OF U.S. EXPORT REGULATIONS

EXECUTIVE SUMMARY

Development of cryptographic products outside the United States is not only continuing but is expanding to additional countries; with rapid growth of the Internet, communications-related cryptography especially is experiencing high growth, especially in electronic mail, virtual private network, and IPsec products. This report surveys encryption products developed outside the United States and provides some information on the effect of the United States export control regime on American and foreign manufacturers.

We have identified 805 hardware and/or software products incorporating cryptography manufactured in 35 countries outside the United States. The most foreign cryptographic products are manufactured in the United Kingdom, followed by Germany, Canada, Australia, Switzerland, Sweden, the Netherlands, and Israel in that order. Other countries accounted for slightly more than a quarter of the world's total of encryption products. A full summary listing of the foreign cryptographic products can be found in an appendix to the report.

The 805 foreign cryptographic products represent a 149-product increase (22%) over the most recent previous survey in December 1997. A majority of the new foreign cryptographic products are software rather than hardware. Also, a majority of these new products are communications-oriented rather than data storage oriented; they heavily tend towards secure electronic mail, IP security (IPsec), and Virtual Private Network applications.

We identified at least 167 foreign cryptographic products that use strong encryption in the form of these algorithms: Triple DES, IDEA, BLOWFISH, RC5, or CAST–128. Despite the increasing use of these stronger alternatives to DES, there also continues to be a large number of foreign products offering the use of DES, though we expect to see a decrease in coming years.

New cryptography product manufacturers have appeared in six new countries since December 1997, and there has been a large increase in the number of products produced by certain countries. The new countries are Estonia, Iceland, Isle of Man, Romania, South Korea, and Turkey. The United Kingdom jumped by 20 products from 119 to 139, and Germany jumped from 76 products to 104. Also notable was Japan's increase, from 6 products to 18, and Mexico's, from a single product to six at the present time.

We identified a total of 512 foreign companies that either manufacture or distribute foreign cryptographic products in at least 67 countries outside the United States. A full summary listing of these is given in an appendix to the report.

On average, the quality of foreign and U.S. products is comparable. There are a number of very good foreign encryption products that are quite competitive in strength, standards compliance, and functionality.

We present sketches of some representative competitors to U.S. manufacturers of software and hardware with encryption capabilities; all are developing products with strong encryption and have as customers a number of large foreign or multinational corporations. The specific companies highlighted are Baltimore Technologies, Brokat, Check Point, Data Fellows, Entrust, Radguard, Seguridata Privada, Sophos, and Utimaco.

We found some examples of advertising used by non-U.S. companies that generally attempted to create a perception that purchasing American products may involve significant red tape and the encryption may not be strong due to export controls. This almost always appeared on Web sites.

We observed that companies vie to have encryption products that meet certain accepted worldwide standards. Encryption experts from all over the world have contributed to two important international standards efforts, IPsec and the Advanced Encryption Standard..

Finally, we suggested that our empirical product data could be combined with economic measures and economic theories to better explain why we are seeing the observed growth and to examine the effects of Internet growth, e-commerce development, and regulatory actions on the international cryptographic market over time, thus getting better insights into the implications of various policy options.

1. INTRODUCTION

This project has three main goals: to provide a comprehensive survey of foreign encryption products available worldwide; to identify specific foreign competitors likely to present a significant economic threat to U.S. manufacturers of software and hardware with encryption capabilities; and to provide evidence, if found, of potential

threats to U.S. leadership in information technology as a result of U.S. export regulations on encryption products.

While this work was undertaken within a very short time frame, and with limited resources, it still provides much new evidence to support the conclusions in Section 7. This evidence can be augmented with additional information as time permits. We do not offer opinions or analysis of key escrow or recovery policies, do long-term technological forecasting, or offer detailed political/social analysis of export control policies. Our goal is to provide an accurate, up-to-date survey of encryption products developed outside the United States and to provide some information on the United States export control regime and its effect on American and foreign manufacturers.

2. PRIOR WORK

One of our first tasks in this project was to examine prior relevant work. Several important documents were studied in this regard.

2.1 U.S. Department of Commerce/National Security Agency Study

The U.S. Department of Commerce Bureau of Export Administration (BXA) and the National Security Agency (NSA) jointly issued a study [Commerce/NSA Study 1996] that assessed the then current and future market for software products containing encryption and the impact of export controls on the U.S. software industry. Quoting from the press release that accompanied the study, ". . . The study found that the U.S. software industry still dominates world markets. In those markets not offering strong encryption, U.S. software encryption remains the dominant choice. However the existence of foreign products with labels indicating DES (Data Encryption Standard) or other strong algorithms, even if they are less secure than claimed, can nonetheless have a negative impact on U.S. competitiveness. The study also notes that the existence of strong U.S. export controls on encryption may have discouraged U.S. software producers from enhancing security features of general purpose software products to meet the anticipated growth in demand by foreign markets. All countries that are major producers of commercial encryption products were found to control exports to some extent. The study found that because customers lack a way to determine actual encryption strength, they sometimes choose foreign products over apparently weaker U.S. ones, giving those foreign products a competitive advantage." [U.S. DoC 1996]

2.2 National Research Council CRISIS Report

A report [CRISIS 1996] was published in 1996 by the National Research Council's Committee to Study National Cryptography Policy. It examined a number of issues related to our study. Based on work by a committee chaired by former Deputy Secretary of State Kenneth Dam and populated by a number of professionals from the law, intelligence, and computer science communities, it concluded that the United States should promote widespread commercial use of technologies that can prevent unauthorized access to electronic information, that the export of the Data Encryption Standard (DES) should be allowed to provide (what was then considered)-an acceptable level of security, and that the United States should progressively relax but not eliminate export controls.

The report also states "widespread commercial and private use of cryptography in the U.S and abroad is inevitable in the long run and its advantages, on balance, outweigh the disadvantages". The committee concludes by noting "the interests of the government and the nation would be best served by a policy that fosters a judicious transition toward a broad use of cryptography".

2.3 President's Export Council Subcommittee on Encryption Report

The President's Export Council Subcommittee on Encryption (PECSENC) is chartered by the Secretary of Commerce to provide the private and public sector with the opportunity to advise the U.S. Government on the future of commercial encryption export policy. The members of the PECSENC consist of representatives from industry, academia, nonprofit foundations, state and local law enforcement, and elsewhere in the private sector. In Septemberl998, its Working Group on International Issues issued a report [PECSENC 1998, included as Appendix D] that found "the difference between U.S. encryption controls and those of other nations is a serious—but not the only—factor determining success in the computer security market." It also concluded that, "the adverse impact of controls on U.S. industry is palpable. For many software applications, business customers simply demand security and encryption; it is a checklist item, and its absence is a deal breaker."

The report also highlighted an example of a non-U.S. company using the difference in export control regimes as "leverage" to ultimately attempt to dominate particular applications:

". . . Brokat, a German company that scarcely existed four years ago, now has 250 employees and offices in several countries including the United States. Brokat's specialty is Internet banking and electronic commerce, but it broke into that business on the strength of being able to offer stronger encryption than German banks could obtain in Netscape or Microsoft browsers. It is now a major player in this niche, with 50% of the European Internet banking market and enough U.S. customers to justify a 20-person U.S. branch office. Meanwhile, encryption constitutes 10% or less of Brokat's revenue, and it has expanded its initial Internet banking offerings to include support for other forms of electronic commerce. Loss of U.S. competitiveness in the electronic commerce software market obviously raises concerns not just about encryption software but other software opportunities. Indeed, it foreshadows a weakening of the U.S. position as a leader in electronic commerce generally."

The report also was concerned that "the persistent emphasis in U.S. export control policy over the past two years on key recovery, or "lawful access," has also taken a toll on the credibility of U.S. security products. . . . Foreign governments and competitors, particularly in Europe, have misinterpreted this U.S. policy, perhaps deliberately. In essence, foreign customers are told often by their governments as well as local security companies that all U.S. encryption products come with a back door allowing the U.S. government to read the contents. In part this is the result of outmoded 'Recovery' supplements to U.S. export rules that demand an unrealistic level of U.S. government access to key recovery products."

3. SURVEY OF CRYPTOGRAPHIC PRODUCTS OUTSIDE THE U.S.

3.1 Overview

The principal investigator and the subcontractor of this current project also studied the worldwide availability of cryptographic products since April 1993 as part of what has become known as the "TIS Survey" [TIS 1997]. The results of this earlier work have been presented to the Computer Systems Security and Privacy Advisory Board (CSSPAB) of the National Institute of Standards and Technology (NIST) and presented by Stephen T. Walker, President of Trusted Information Systems, to two Congressional subcommittees [Walker 1993, Walker 1994]. The survey was also provided to numerous government agencies and departments as part of their efforts to understand the availability of cryptographic products and its impact on U.S. export control policies.

The TIS Survey continued until December 1997, at which time it identified 656 foreign cryptographic products from 29 countries. The survey also identified 963 domestic products, for a worldwide total of 1619 products produced and distributed by 949 companies (474 foreign and 475 domestic) in at least 68 countries.

Our goal for this current study was to update the foreign product portion of the TIS Survey. We focused mainly on discovering new products from foreign manufacturers and also spent some time updating entries for the existing foreign products in the database.

Information collected by the TIS Survey was assembled into an MS Access database. The database includes two tables, one for cryptographic products and a second table for companies that either produce or distribute cryptographic products. Each entry in the product table includes the following information: Name/Version, Manufacturer and Country, Platforms:

- PC, Mac, Workstation, Mainframe, DOS, Windows, UNIX, etc., Interfaces;
- RS232, X.21, X.25, V.21, V.24, RJ-11, etc., Type;
- HW, SW, HW/SW combo, What It Encrypts;
- Data, Files, Directories, Disks, Communications, Voice, Fax, Tape, Email, etc., Embodiment;
- Program, Kit, Chip, Board, Box, Tokens, PCMCIA, Smart Card, Phone, etc. Cryptographic Algorithms;
- DES, Triple DES (3DES), Blowfish, IDEA, CAST, Proprietary, RC2/4/5, SKIPJACK, Stream Ciphers, RSA, El Gamal, DH, DSA, ECC, MD2/4/5, SHA–1, etc., How Distributed;
- Mass-Market, Direct, Shareware, Internet, etc., Company Information;
- Name, Country, Address, Contact Information, etc.

3.2 Data Collection Methodology

We used the following methods of data collection: issue a call for information and examine the results, plumb existing work available to us, and use the World Wide Web to conduct searches for new products and information.

The call for information to elicit information from the computer cryptography community regarding new products (Appendix A) was posted in the following newsgroups and mailing lists (IETF is the Internet Engineering Task Force [IETF]):

- sci.crypt newsgroup: discussion of the science of cryptology, including cryptography, cryptanalysis, and related topics such as one-way hash functions.
- Risks mailing list: describes many of the technological risks that happen in today's environment.
- Cypherpunks mailing list: forum for discussing cryptography, privacy, and related social issues.
- Cryptography mailing list: mailing list devoted to cryptographic technology and its political impact.
- Firewalls mailing list: discussion of Internet "firewall" security systems and related issues.
- IETF Web Transaction Security (wts) Working Group mailing list: discussion of the development of requirements and a specification for the provision of security services to Web transaction.
- IETF Secure Shell (secsh) Working Group mailing list: discussion of efforts to update and standardize the SSH protocol.
- IETF IP Security Protocol (ipsec) Working Group mailing list: discussion of the standards efforts on IP Security.
- IETF An Open Specification for Pretty Good Privacy (openpgp) Working Group mailing list: discussion of extending the current PGP protocol.

The Call and Survey were also posted on the Web site of the Cyberspace Policy Institute of The George Washington University [CPI 1999]. Additionally, project team members sent the survey out to individuals who they believed might know of foreign products.

The existing work available to us included trade magazines, journals, buyers guides [CSI, ICSA Survey], and other print material.

Most of our new information on foreign cryptography products was found by using Web search engines and gathering information from Web pages.

3.3 Results of Update to Cryptographic Products Survey

Our effort to update the cryptographic products survey focused mainly on discovering new products from foreign producers, but also involved updating information on some of the existing foreign products in the database. Since we did not set out to update information on cryptographic products produced in the U.S., the number of domestic cryptographic products changed only slightly (when we came across something and thus updated the information). However, we expect that the number of cryptographic products produced in the U.S. has in fact also increased. NAI Labs plans to further update the domestic portion of the survey in the near future.

The updated foreign cryptographic product survey (see summary table on following page) now identifies a total of 805 hardware and/or software products incorporating cryptography manufactured in 35 countries outside the United States. The most foreign cryptographic products are manufactured in theUnited Kingdom, followed by Germany, Canada, Australia, Switzerland, Sweden, the Netherlands, and Israel in that order. Other countries accounted for slightly more than a quarter of the world's total of encryption products. A full summary listing of the foreign cryptographic products can be found in Appendix B.

The 805 foreign cryptographic products resulting from the current update represents a 149-product increase over the December 1997 survey. A majority of the new foreign cryptographic products are software rather than hardware.

Another notable finding is that a majority of new foreign cryptographic products are oriented toward communications rather than data storage applications; and these heavily tended towards secure electronic mail, IP security (IPsec), and Virtual Private Network (VPN) applications. The results also showed a lot of activity in IPsec implementation, which is likely prompted by the recent emergence of new IPsec specifications from the IETF [IPSEC].

The updated foreign cryptographic product survey also identified a total of 512 foreign companies that either manufacture or distribute foreign cryptographic products in at least 67 countries outside the United States. A full summary listing of these is given in Appendix C.

3.3.1 More "Strong" Encryption is on the Market

The updated foreign cryptographic products survey also showed increasing use of "strong" alternative cryptographic algorithms to DES, which uses a 56-bit key. Altogether, we identified at least 167 foreign cryptographic products that use Triple DES, IDEA, BLOWFISH, RC5, or CAST-128, which support larger key lengths. Despite the increasing use of these stronger altematives to DES, there also continues

to be a large number of foreign products offering the use of DES, though we expect to see a decrease in coming years.

We identified at least 123 foreign cryptographic products that use Triple DES, which employs either two traditional DES keys, for an effective key length of 112 bits, or three DES keys, for an effective key length of 168 bits.

We identified at least 54 foreign cryptographic products that use the International Data Encryption Algorithm (IDEA), a Swiss-developed symmetric block cipher with a 128-bit key length [Lai 1990, Lai 1991].

We identified at least 36 foreign cryptographic products that use BLOWFISH, a symmetric block cipher developed by Bruce Schneier with a variable key length ranging from 32 to 448 bits [Schneier 1993, Schneier 1994]. Many of these products appear to use BLOWFISH with the full 448-bit key length.

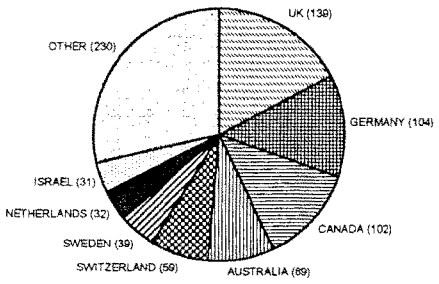
We identified at least 2 foreign cryptographic products that use RC5, a symmetric block cipher developed by Ron Rivest (one of the RSA inventors) with a variable length key up to 2040 bits [Rivest 1996].

We identified at least 12 foreign cryptographic products that use CAST-128, a symmetric block cipher developed by Carlisle Adams of Entrust Technologies in Canada with a variable length key up to 128 bits [Adams 1997].

Foreign Cryptographic Survey Results (as of May 1999)

The updated survey identified a total of 805 foreign cryptographic products from 35 countries:

Argentina	Australia	Austria
Belgium	Canada	Czech Republic
Denmark	Estonia	Finland
France	Germany	Greece
Hong Kong	Iceland	India
Iran	Ireland	Isle Of Man
Israel	Italy	Japan
Mexico	Netherlands	New Zealand
Norway	Poland	Romania
Russia	South Africa	South Korea
Spain	Sweden	Switzerland
Turkey	UK	



At least 167 of these foreign cryptographic products implement "strong" cryptographic algorithms, including Triple DES, IDEA, BLOWFISH, RC5, or CAST.

We identified 512 foreign cryptography companies (including distributors as well as manufacturers) in at least 67 countries.

Table 1. Foreign cryptographic products survey results

3.3.2 New Countries and Growth Countries for Cryptographic Products

The update identified six new countries producing cryptographic products. The countries that have started producing encryption products since December 1997 are Estonia, Iceland, Isle of Man, Romania, South Korea, and Turkey.

We also noticed a large increase in the number of products produced by certain countries, such as the United Kingdom, which jumped by 20 products from 119 to 139, and Germany, which jumped from 76 products to 104.

Japan also showed a large increase, jumping from 6 products in the December 1997 survey to 18 products in the updated survey. Most of the new products come from Mitsubishi Electronic Corporation, which has introduced a number of hardware and software cryptographic products that make use of a Japanese cryptographic algorithm known as MISTY, which uses a 128-bit key as well as Triple DES [Matsui 1996, MISTY].

Mexico also increased, from a single "freeware" product in the December 1997 survey to six products in the updated survey, due to the discovery of five new commercial cryptographic products from Seguridata Privada S.A de C.V., which is described in greater detail in Section 4.

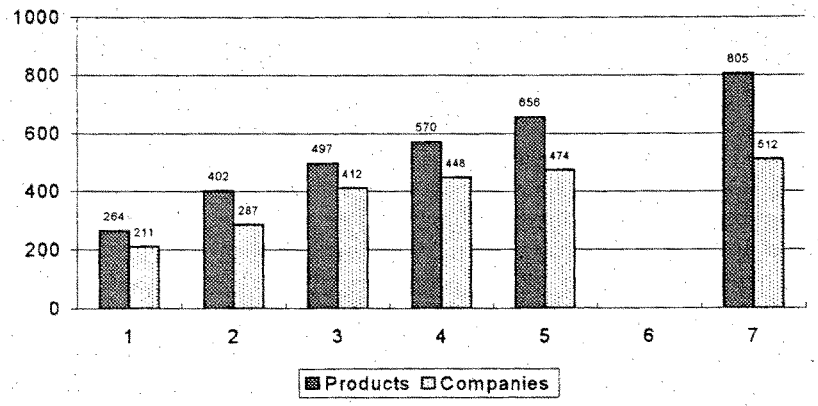


Figure 2. Growing numbers of foreign cryptographic products and companies

3.3.3 Growing Numbers of Foreign Products & Companies

The TIS Survey was initiated in April 1993 and conducted on an ongoing basis through December 1997. Figure 2 depicts the evolution of the survey in terms of the increasing numbers of foreign cryptographic products and companies (manufacturers and distributors) identified each year of the survey effort and after the recent update. Overall, there clearly continues to be increasing and expanding development of foreign cryptographic Products.

3.3.4 Quality of Foreign Cryptographic Products

NAI Labs has obtained a number of foreign cryptographic products over the life of the survey effort. The products were all purchased via routine channels, either directly from the foreign manufacturer, a foreign distributor, or an U.S. distributor. We have also downloaded a large number of foreign cryptographic products over the Internet via the World Wide Web.

The quality of cryptographic products varies greatly both within and outside the U.S. We have encountered poor quality products both within and outside the U.S., and we have encountered good quality products both within and outside the U.S. On average, the quality of foreign and U.S. products is comparable. There are a number of very good foreign encryption products that are quite competitive in strength, standards compliance, and functionality. We highlight some of these in the next section.

4. SOME COMPETITORS TO U.S. PRODUCTS EMPLOYING CRYPTOGRAPHY

After updating the cryptography product database, based on prior surveys and new information, we searched out information on the foreign manufacturers that were representative competitors to U.S. manufacturers of software and hardware with encryption capabilities. We did this by examining traditional sources such as business magazines, major newspapers, and trade publications; interviewing industry leaders and security professionals; and using various Web-based search methods [Lexis-Nexis, ABI/Inform, FirstSearch, Gale] to find appropriate combinations of keywords (encryption, U.S., US, United States, foreign, overseas, regulation, export, export controls).

We identified a substantial number of foreign companies that are developing a number of products with strong encryption and have as customers a number of large foreign or multinational corporations. We sketch nine of these in this section to provide a representative sampling. All but one already provide strong encryption (as defined in Section 3.3.1).

Some of the material below has references to cryptographic algorithms, protocols, and other computer science terms that may not be familiar to some readers. More information on these can generally be found in [Stallings 1999] and [Rivest 1978].

Baltimore Technologies Plc, IRELAND / UNITED KINGDOM / AUSTRALIA

Baltimore Technologies plc. was formed by the merger in January 1999 of Zergo Holdings plc. (UK) and Baltimore Technologies Ltd. (Ireland). Its regional headquarters are located in Dublin (Ireland), Plano (Texas) and Sydney (Australia). Corporate headquarters are located in London, UK [Baltimore 1999a].

Baltimore develops and markets security products and services for a wide range of e-commerce and enterprise applications. Its products include Public Key infrastructure (PKI) systems, cryptographic toolkits, security applications and hardware cryptographic devices.

Baltimore's security toolkits include PKI-Plus, ECS Desktop, C/SSL, J/SSL, SMT, CST, and J/CRYPTO. The PKI-Plus toolkit provides clients with the functionality to support a Public Key Infrastructure and provides encryption capabilities with full strength DES, Triple DES and IDEA. ECS Desktop is a high level GSS toolkit that supports 64-bit DES and 128-bit Triple DES. C/SSL and J/SSL are cryptographic toolkits for developing SSL 3.0 applications written in C and Java respectively. C/SSL supports 56-bit DES and 128-bit Triple DES, IDEA and RC4. J/SSL supports 56-bit DES, and 128-bit Triple DES and RC4. SMT (Secure Messaging Toolkit) provides developers the ability to add security to messaging (email) applications. The encryption algorithms supported are 56-bit DES, 128-bit Triple DES, and 40-bit, 64 bit, and 128-bit RC2. CST (Crypto Systems Toolkit) is a set of cryptographic components enabling developers to build strong information security systems. It contains implementations of a variety of encryption algorithms including DES, Triple DES with up to 192 bits key length, IDEA, BSA4, BSA5, RC2, RC4, up to 2048-bit RSA, and DSA. J/CRYTPO is a cryptographic class library for Java applications that supports 56-bit DES, 112-bit Triple DES, and RC4 encryption, and 512-, 1024-, and 2048-bit RSA key exchange and digital signature.

Security application solutions include FormSecure, MailSecure, MailSecure Enterprise, and WebSecure. Of its security applications, FormSecure which provides PKI security for Web browser forms uses DES and triple-DES encryption with 128-bit keys. MailSecure provides secure email for MS Outlook, Exchange and Eudora using 128-bit DES, Triple DES and RC2. MailSecure Enterprise, a centralized secure email product, provides encryption with 128-bit Triple DES. WebSecure enhances web server to browser communication in eases where export versions of specific browsers are limited to 40 bits of encryption by diverting all web traffic to its Java programs that use 128-bit RC4 encryption.

Baltimore's hardware cryptographic device, HS4000-Assure provides a security kernel for high speed servers and workstations and features 56-bit DES and 112-bit Triple DES data encryption, and up to 4096-bit RSA key exchange and digital signatures.

"Baltimore has customers in over forty countries including some of the world's leading financial, e-commerce, telecommunications companies and government agencies. Customers include: ABN-AMRO Bank, Australian Tax Office, Bank of England, Bank of Ireland, Belgacom, Digital Equipment, European Commission, Home Office (UK), IBM, Lehman Brothers, Ministry of Defense (UK), NatWest, NIST (USA), PTT Post (Netherlands), S.W.I.F.T., Tradelink (Hong Kong), TradeVan (Malaysia) and VISA International" [Baltimore 1999a] .

"Baltimore has also formed alliances with other major global providers of information security technology and services, including ActivCard, Axent Technologies, CDC, Certicom, Chrysalis, CISCO, Dascom, DataKey, GemPlus, Gradient, Hewlett-Paekard, ICL, Isocor, Kyberpass, Logica, Netseape, Oracle, Racal and Valicert" [Baltimore l999a].

Brokat Infosystems AG, GERMANY

BROKAT was founded in 1994. Its headquarters is in Stuttgart, Germany. Subsidiaries are located in Great Britain, Ireland, Luxembourg, Austria, Switzerland, Singapore, Australia, South Africa and the United States. Brokat develops secure solutions for Internet-banking, Internet-brokerage and Internet-payment by allowing companies through the use of its products to develop secure electronic banking and electronic commerce solutions [Brokat l999a]. Its main product, Brokat Twister, is a software package enabling secure electronic business solutions and provides Java-based 128-bit encryption. Brokat's X-PRESSO Security Gateway provides Twister with a secure Internet channel, using strong SSL encryption. It supports 128-bit IDEA and Triple DES for data encryption, and RSA up to 2048 bits for key exchange and digital signatures.

In its press release of May 19, 1999 Brokat claims a sales increase of 125% in the third quarter of 1998/1999 compared to the same quarter in the previous year [Brokat 1999b].

More than 100 financial service companies use Twister. Brokat customers include Deutsche Bank, Bank 24, Allianz, Fortis Bank Luxembourg the Zurich Kantonalbank, Hypo Bank of Munich, and The Swiss National Telephone Company [Andrews 1997].

Brokat's "Product Partners" include AOL Bertelsmann Online, Corporate Interactive, Inc., Intershop Communications, Micrologica, Netscape Communications, Giesecke & Devrient, and Concord-Eracom.

Check Point Software Technologies Ltd., ISRAEL

"Check Point provides secure enterprise networking solutions through an integrated architecture that includes network security, traffic control and IP address management. Check Point solutions are aimed at enabling customers to implement centralized policy-based management with enterprise-wide distributed deployment" [Check Point 1999a].

"The company's integrated architecture includes network security (FireWall–1, VPN–1, Open Security Manager and Provider–1), traffic control (FloodGate–1 and ConnectControl) and IP address management (Meta IP)" [Check Point 1999b].

"Check Point products protect and manage the corporate assets of the majority of Fortune 100 companies and other leading companies and government agencies across the globe. As of April 1999, the company had more than 30,000 registered customers with over 77,000 installations worldwide and 17,000+ networks worldwide using its VPN solution. The Meta IP and Meta DNS products had some 15,000 installations worldwide" [Check Point 1999b].

The company's international headquarters are located in Ramat-Gan, Israel. International subsidiaries are located in the United Kingdom, France, Germany, Japan, Singapore, Australia, the Middle East and Canada. U.S. subsidiaries are located in northern and southern California, Colorado, Georgia, Illinois, Massachu-

setts, Michigan, New York, North Carolina, Philadelphia, Texas, Virginia and Washington.

In an April 19, 1999 press release, Check Point announced that "revenues for the first quarter ending March 31 were $43,772,000 compared to $31,956,000 for the same period in 1998, an increase of 37%. Net income for the quarter was $19,703,000, or $0.49 per share compared to net income of $15,149,000, or $0.39 per share in the same quarter in 1998, an increase of 30% in net income and 26% in net income per share. Check Point experienced growth across all geographic regions, particularly in Japan. Revenues from the U.S. accounted for 45% of revenues, Europe 34% and Rest of World 21%. In addition, revenues from Technical Services reached 17% in the first quarter. OEM revenues, including those from Nokia and Sun Microsystems, represented 11% of revenues" [Check Point 1999c] .

Based on figures from 1997, Check Point is the leading vendor of firewalls with a 23% share in the firewall market—a revenue of $83 million in firewall sales [Inter@ctive Week 1998].

Checkpoint's firewall solution, Firewall–1 provides a comprehensive set of security solutions which includes VPN through the support of encryption algorithms such as 40- and 56-bit DES, 168-bit Triple DES, 40-bit RC4, 40- and 128-bit CAST, and 48-bit FWZ–1 (FWZ–1 is Check Point's 48-bit exportable proprietary symmetric encryption algorithm).

Check Point's VPN solution products include VPN–1 Gateway, VPN–1 SecuRemote, VPN–1 Accelorator Card, and VPN-1 Appliance. VPN–1 Gateway products are software solutions that provide encryption supporting the following algorithms: 40- and 56-bit DES, 168-bit Triple DES, 40-bit RC4, 40- and 128-bit CAST, and 48-bit FWZ–1. VPN–1 SecurRemote provides VPN support for remote and mobile users. It supports 40- and 56-bit DES, 168-bit Triple DES, 40-bit CAST, and 48-bit FWZ–1. VPN–1 Accelorator Card provides hardware-based data encryption using 56-bit DES and 168-bit Triple DES. VPN–1 Appliance uses 40-and 56-bit DES, 40-bit RC4, and 48-bit FWZ–1.

Check Point's Open Platform for Secure Enterprise Connectivity (OPSEC) is an alliance that delivers the industry's first enterprise-wide security framework. OPSEC provides a single framework that integrates and manages all aspects of secure enterprise networking through an open, extensible management framework Via the OPSEC Alliance, Check Point Software's products seamlessly integrate with "best-of-breed" products from more than 200 leading industry partners. A complete listing of OPSEC partners can be found at http://www.opsec.com/.

Data Fellows Ltd., FINLAND

"Data Fellows develops, markets and supports data security products for corporate computer networks. Its products include anti-virus software, and data security and cryptography software. Its main offices are in San Jose, California and Espoo, Finland, and it has branch offices as well as corporate partners, VARs and other distributors in over 80 countries around the world. Its products have been translated into over 20 languages" [Data Fellows 1999a].

Data Fellows' F-Secure cryptography products are a family of cryptography software to protect the integrity and confidentiality of sensitive information. Its family of products include F-Secure VPN+, F-Secure VPN, F-Secure SSH, F-Secure FileCrypto, and F-Secure Desktop. F-Secure VPN+ provides IPSec protocol based security for secure networking between remote offices, business partners and travelling salesmen using 56-bit DES, 168-bit Triple DES, 128-bit Blowfish, and 128-bit CAST. F-Secure VPN (Virtual Private Network) is an SSH security protocol based solution for pure LAN-to-LAN encryption using a variety of user selectable algorithms including Triple DES, Blowfish, RSA, and IDEA (optional). The symmetric algorithms all use at least 128 bits. F-Secure SSH Server provides users with secure login connections, file transfer, X11, and TCP/IP connections over untrusted networks using 128-bit Triple DES and 128-bit IDEA. F-Secure SSH Terminal&Tunnel provides the user with secure login connections over untrusted networks and to create local proxy servers for remote TCP/IP services. F-Secure SSH Tunnel&Terminal products support the following cryptographic algorithms: 56-bit DES, 168-bit Triple DES, 128-bit IDEA, 128-bit Blowfish, 256-bit Twofish, and 128-bit ARCFour (an RC4 compatible stream cipher). F-Secure FileCrypto is a product that encrypts and decrypts files using 256-bit Blowfish and 168-bit Triple DES. F-Secure Desktop provides encryption and decryption of files, directories, and Windows 95/NT 4.0 folders using 256-bit Blowfish and 168-bit DES.

"The Company's net sales have doubled annually since it was founded in 1988. Turnover has reached $3.3 million, $7.6 million and $14.1 million in the fiscal years 1995, 1996 and 1997, respectively" [Data Fellows 1999a].

"Data Fellows has customers in more than 100 countries. These include many of the world's largest industrial corporations and best-known telecommunications companies; major international airlines; several European governments, post offices and defense forces; and several of the world's largest banks. Customers include NASA, the US Air Force, the US Department of Defense Medical branch, the US Naval Warfare Center, the San Diego Supercomputer Center, Lawrence-Livermore National Laboratory, IBM, Unisys, Siemens-Nixdorf, EDS, Cisco, Nokia, Sonera (formerly Telecom Finland), UUNet Technologies, Boeing, Bell Atlantic, and MCI" [Data Fellows 1999a].

Entrust Technologies, CANADA

Entrust is a Canadian company that spun off from Northern Telecom (Nortel). It develops cryptographic products in Canada and exports them from there. It now has offices across the United States, Canada, the United Kingdom, Switzerland, Germany, and Japan.

Entrust develops products for trusted electronic transactions. Its products include solutions for secure Internet transactions including digital certificate services and public-key infrastructures (PKI) products.

Entrust File Toolkit delivers a set of application programming interfaces (APIs) to add encryption and digital signatures to store-and-forward (email, e-forms) applications. It Supports DES, Triple DES, RSA and RC2. Entrust Session Toolkit is designed for third-party applications that need to protect data communications in real-time. It supports DES, Triple DES, and RC2. Entrust/Solo is a product that provides data encryption, digital signature and data compression functionality for the desktop and e-mail using DES, Triple DES and CAST.

The company's more than 800 corporate customers include J.P. Morgan, the Salomon Smith Barney unit of Citigroup, ScotiaBank, S.W.I.F.T, FedEx, the Canadian Government and several U.S. government agencies.

Entrust's industry partners include development partners such as Hewlett-Packard, Network Associates, Oracle, Nortel Networks and others, 25 channel partners including Hewlett-Packard and Compaq OEM Partners: IBM, Tandem, Check Point and others, specifiers and referral partners such as PriceWaterhouse Coopers, Deloitte & Touche; KPMG Peat Marwick, Ernst & Young, and others, and service provider partners such as BCE Emergis, EDS, Scotiabank and others [Entrust 1999].

Radguard, ISRAEL

RADGUARD was founded in 1994 as a member of the RAD Group of data communications companies. Privately held, the company is backed by American and foreign corporate investors. The company's international headquarters are located in Tel Aviv, Israel; its US headquarters are in Mahwah, NJ.

Radguard is a pioneer and leader in the secure Virtual Private Network (VPN) market. Incorporating security technologies and industry standards into high-performance hardware architectures, Radguard provides solutions to Internet-based virtual private networking, secure non-Internet transmission, safe Internet connectivity and client encryption. Its VPN and network security products include cIPRO, CryptoWall, and NetCryptor. cIPRO is an Internet-working security system for VPNs. The cIPRO family uses DES and up to 168-bit Triple DES for encryption. CryptoWall is an encrypting firewall that supports subnet-to-subnet security in TCP/IP environments. It supports DES for data encryption and RSA for key exchange and digital signature. NetCryptor is a hardware-based encryption device that employs DES.

Customers include NTT Data, a subsidiary of Japan's Nippon Telephone and Telegraph (NTT), Germany's major car makers and component suppliers including BMW, Bosch, BEHR, Drëxlmaier, Audi, Freudenberg, DaimlerChrysler, Volkswagen and Hella.

Seguridata Privada S.A de C.V., MEXlCO

SeguriDATA is a Mexican company founded in 1996 with the purpose of participating actively in the construction of security standards in Mexico and Latin America by means of integration in committees, with products in electronic security. It has offices in Peru and Spain as well as Mexico. The company provides confidentiality and authenticity of electronic documents with applications to electronic commerce, financial transactions and confidential systems of communications.

Its products include SeguriDOC, SeguriEDIFACT, SeguriLIB, SeguriPROXY, and SeguriTELNET. SeguriDOC offers Triple DES for confidentiality of archived data. SeguriEDIFACT provides security for EDI communications using Triple DES. SeguriPROXY provides security between web server and web browser sessions using 128-bit RC4.

Sophos Plc., UK

Sophos Plc was founded in 1980 and moved into data security in 1985, producing software and hardware for data encryption, authentication and secure erasure. Its virus detection product has positioned the company as a leading supplier of enterprise-wide virus protection tools. Subsidiaries include Sophos Pty Ltd, Australia, established in April 1999, Sophos Plc, France, established in May 1998, Sophos GmbH, Germany established in October 1997, and Sophos Inc, USA, a wholly-owned subsidiary of Sophos Plc based in Massachusetts, USA [Sophos 1999]. Sophos data security products include D-Fence 4 HMG, D-Fence 4 SPA, E-DES, and PUBLIC. D-FENCE HMG is a disk authorization and encryption system for HMG, providing encryption and authentication of floppy and hard disks using SEVERN BRIDGE, a U.K. Government standard algorithm. D-FENCE SPA is a data encryption system for PCs and laptops using SPA (Sophos Proprietary Algorithm) for encryption of floppy and hard disks. SPA is a 64-bit block cipher with 64-bit keys. E-DES and PUBLIC are products used for secure file storage and transmission. E-DES encrypts files using DES or SPA, while PUBLIC encrypts files using 512-bit RSA or MDH in combination with DES or SPA.

Customers include government, financial institutions and multi-national corporations.

Utimaco Safeware AG, GERMANY

Utimaco Safeware AG has subsidiaries in Belgium, France, Finland, Great Britain, Austria, the Netherlands, Norway, Sweden and Switzerland and additional distribution partners (Value-Added-Resellers) in almost all European countries, in the USA, Australia, Asia and in South Africa. Utimaco also has strategic alliances with IBM Deutschland Informationssysteme GmbH, SIEMENS AG and Toshiba Europe.

Utimaco develops IT security solutions for the areas of mobile/desktop security (authentication, access control, encryption), network security (authentication, encryption), e-commerce security (digital signature, encryption) and security infrastructure (smart card reader).

"Utimaco has three development centres. The SafeGuard product line focussing on the "Mobile/Desktop Security" area is developed in Munich, Germany. The development of the SafeGuard product family for "Network Security" and the smart card technology and card reader family CardMan is done in Linz, Austria. The third development centre near Brussels (Holsbeck), Belgium, is responsible for the SafeGuard "E-Commerce Security" product line (digital signatures, e-mail security) and the CriptWare technology (high-performance implementations of standardized basis-crypto algorithms and interfaces)" [Utimaco 1999a].

Products for mobile/desktop security include SafeGuard Easy, and SafeGuard Desktop. SafeGuard Easy is a security program for the online-encryption of hard disks and diskettes. It operates with the encryption algorithms Blowfish, STEALTH, 56-bit DES and 128-bit IDEA to guarantee the confidential storage of sensitive data. SafeGuard Desktop is a security solution for OS/2 operating systems offering boot and virus protection as well as user logon, and allows online encryption of hard disks and floppies with DES, IDEA, STEALTH, Blowfish, and XOR.

Utimaco network security products include SafeGuard LAN Crypt and SafeGuard VPN. SafeGuard LAN Crypt provides protection of selected files against access by persons who are physically capable of accessing the data carrier. The solution guarantees the security of encrypted data through a key length of 128 bits and globally accepted, strong algorithms such as IDEA. SafeGuard VPN provides Virtual Private Networks with secure data transmission using 168-bit Triple DES and 128-bit IDEA.

Utimaco's E-commerce security products include CryptWare Board, CryptWare Server, Cryptware Toolkit, and SafeWare Sign&Crypt. Cryptware Board comes with a DES chip, but allows any other encryption algorithm to be easily installed. The CryptWare Server is a cryptographic black box designed for applications with high security requirements and/or high-speed cryptographic capabilities. It employs DES and 1024-bit RSA. The CryptWare Toolkit is a library that provides all necessary cryptographic and administrative functions to build secure electronic messaging systems. It supports RSA, Triple DES, IDEA, RIPEMD160, MD5, and SHA–1. SafeWare Sign&Crypt offers signing and verification of electronic documents. It can provide encryption with 128-bit IDEA.

The breakdown of Utimaco Group sales by industry in the last business year, 1997/98, is as follows: 29.7% for public institutions, 29.3% for banks, 26.8% for industry and commerce and 14.1% for insurance companies. In the last business year 57 percent of sales were made outside Germany. Its customers include Bertelsmann (Gutersloh) Colonia Nordstern Versicherungsmanagement AG (Cologne), Daimler-Benz Aerospace AG (Kiel), Dresdner Bank, Eduscho GmbH (Bremen), Frankfurter

Sparkasse (Frankfurt), Goldwell GmbH (Darmstadt), Innenministerium Mecklenburg-Vorpommem (Schwerin), Landesamt fur Datenverarbeitung, (Potsdam), Motorola GmbH (Taunusstein), Otto Versand International GmbH (Hamburg), Oberverwaltungsgericht Thuringen (Weimar), Price Waterhouse (Frankfurt), Police Forces (Belgium), Isaserver (Belgium), State Police (Belgium), Unisys for Christelijke Mutualiteiten (Belgium), The European Commission (Belgium and Luxembourg), Danfoss A/S (Denmark), ICL Pathway Ltd. (Great Britain), Robert Fleming & Co. Ltd. (Great Britain), Standard Chartered Bank (Great Britain), Conseil de I Union Europeenne (Luxembourg), KPN Telecom (The Netherlands), ABN AMRO Bank N.V. (The Netherlands), Nycomed Amersham Group (Norway), Schweizer Post (Switzerland), DDJ, and Justizdirektion des Kantons Zurich (Switzerland).

5. FOREIGN MARKETING USE OF U.S. EXPORT CONTROLS

5.1 Introduction

As Under Secretary of Commerce William A. Reinsch noted in recent Congressional testimony, "encryption remains a hotly debated issue. The Administration continues to support a balanced approach that considers privacy and commerce as well as protecting important law enforcement and national security equities. We have been consulting closely with industry and its customers to develop a policy that provides that balance in a way that also reflects the evolving realities of the market place" [Reinsch 1999]. As the Commerce Department struggles to craft and finely tune export regulations to satisfy these objectives, many foreign cryptography manufacturers are citing these regulations as reasons for their prospects to not "buy American". Even foreign governments sometimes overtly use these regulations. For example, "In a letter sent [in January 1999] to India's Central Vigilance Commission (CVC)—an intelligence agency comparable to the United States' National Security Agency—the Indian Defense Research and Development Organization said the limits the U.S. government places on exported encryption products render the products too weak for reliable use. The CVC responded that it might mandate that all Indian financial institutions buy security software from India" [Dunlap 1999].

5.2 Advertising Related to Cryptographic Controls

Trade magazines, industry reports, and news articles were searched for consumer preference data, including checklists, ease of use" and "best buy" ratings, etc., to try to find anecdotal justification or rebuttal of the claim that consumers strongly prefer U.S.-made encryption products and systems incorporating U.S.-made encryption, as asserted, for example, in [Ernst 1999].

We did find a reference to a U.S. government study that acknowledged that "in many countries surveyed, exportable U.S. encryption products are perceived to be of unsatisfactory quality" [Commerce/NSA 1996] {date given as June 1995, page ES–3, possibly a draft, in [Olbeter 1998]}. We also found some information from companies that claimed or implied that their products are more secure and/or easier to use than American products burdened by U.S. export controls. Descriptions of the various export control regimes are found in [Baker 1998, Koops 1999, and GILC 1998].

Examples of the statements of foreign companies are given below.

Brokat Infosystems AG (Germany)

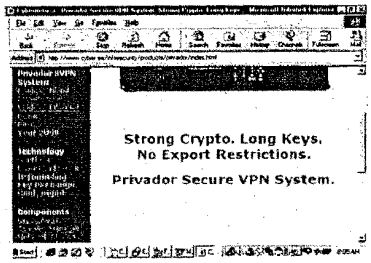
Brokat, on its web page [Brokat 1999c] discusses "Secure Communication using 128-bit encryption" and states that "In comparison to other solutions, X–AGENT allows very secure communication. Highly sensitive information can be exchanged using this consultation tool. All data is encrypted with the 128-bit Twister security component. Even so-called 'weak' Internet browsers, which only use a 40-bit encryption due to US government export restrictions can be 'topped up' accordingly for the duration of the session."

Baltimore Technologies plc. (Ireland/United Kingdom/Australia)

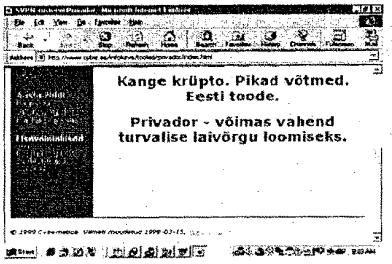
Baltimore Technologies states that WebSecure, a product designed to provide secure web server to browser communication is useful because "US export restrictions dictate that most web servers and browsers cannot perform 128-bit encryption for security. Instead, export versions of browsers like Internet Explorer and Netscape Navigator and export versions of web servers like Netscape Enterprise Server and Microsoft Internet Information Server are limited to 40 bits of encryption, which is not secure enough for most applications" [Baltimore 1999b].

Cybernetica (Estonia)

Cybernetica advertises ". . . full strength cryptographic security with long keys and no backdoors" and its Web pages for their products prominently feature this selling point.



[Cybernetica 1999a]



[Cybernetica 1999b]

In their Frequently Asked Questions list on the Web, they go on to celebrate the differences between their product and U.S. products:

• *Strong crypto? What algorithms are supported? And what key lengths?*

IDEA. Triple DES. Blowfish. RSA. Diffie-Hellman. The end user has the opportunity of selecting the algorithms he trusts. And, if the user so requires, support for further algorithms may be added. You can use as long keys as the algorithms you have selected allow you to. There are no "political" restrictions on key lengths to be used in the Privador system.

• *What about back doors, key recovery etc?*

There are no back doors built into the Privador system. We can—and will—prove It if so required.

• *How come you don't care about export restrictions?*

Because there are none. The Privador System is entirely developed by Cybernetica, the first private-law R&D institution in Estonia. The laws of the Republic of Estonia allow us to export strong cryptographic technologies to almost any country in the world.

Utimaco Safeware AG (Germany)

On its web site, Utimaco states that [Utimaco 1999b] ". . . As a German manufacturer, Utimaco guarantees that no national key depositing requirements (ESCROW) exist which could jeopardize the security of the solution . . ."

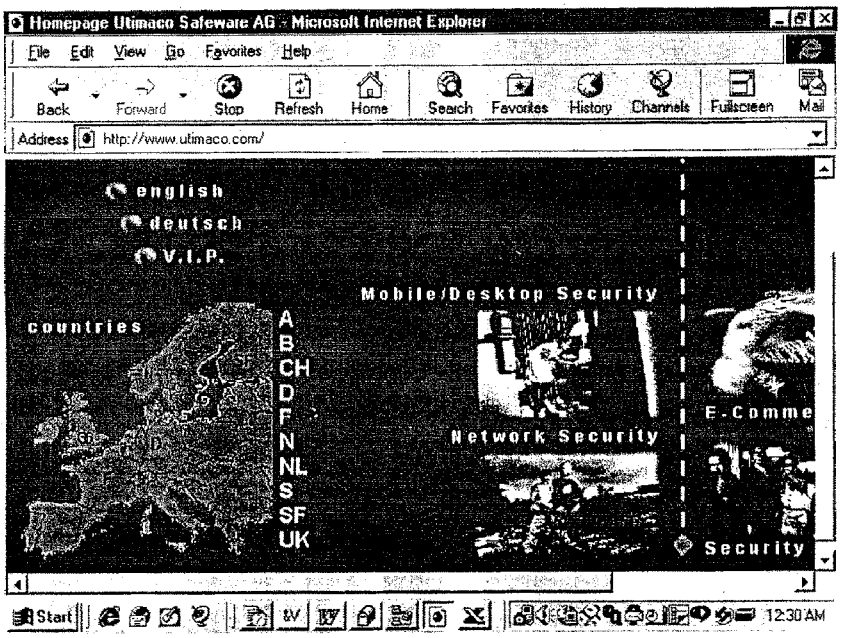


Figure 3. Homepage of Utimaco Safeware AG

Note Utimaco's home page, illustrated in Figure 3. It is user-friendly for speakers of a number of languages. It makes the point that Utimaco has representatives in a number of European countries. If the user clicks on his or her country (either on the map or on the country abbreviation in the vertical list), he or she is transported to a page in their native language that further presents Utimaco and its products and services. As an example, Figure 4 shows the homepage of Utimaco Norway that the user is transported to when Norway is selected from the map.

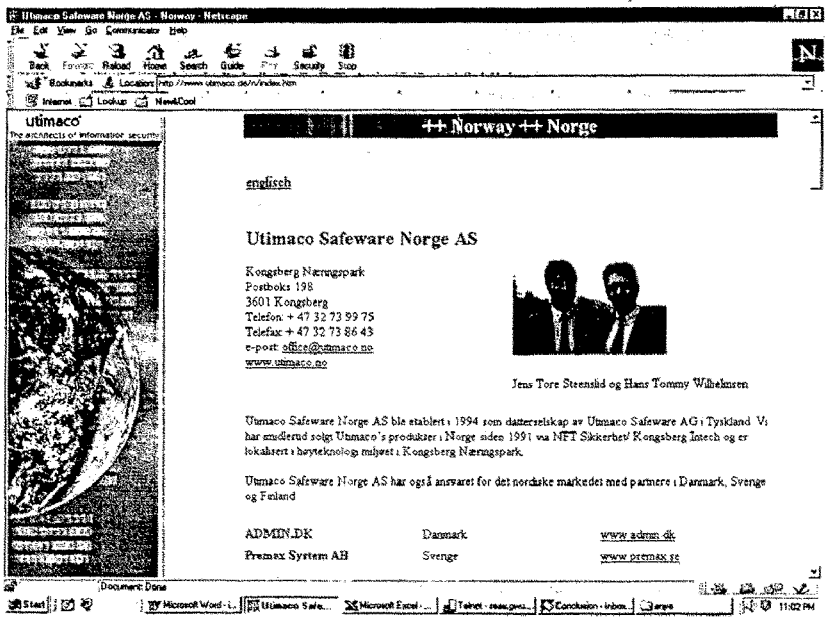


Figure 4. Homepage of Utimaco Safeware Norge AS

Data Fellows Corporation (Finland)

Data Fellows makes the readers of its web page aware of U.S. export restrictions and states that its products are designed with "much more security" than U.S. products:

> ". . . The encryption technology used in the F-Secure products has been developed in Europe and thus does not fall under the US ITAR export regulations. F-Secure products can be used in every country where encryption is legal, including the United States of America . . ." [Data Fellows 1999b]
>
> ". . . F-Secure FileCrypto uses well-known fast block cipher algorithms. You can choose either three-key 3DES or Blowfish. Both algorithms have been analyzed by the world's leading cryptographers. They are known to be strong and safe. These algorithms provide security with a minimum of 168-bit keys. They provide much more security than DES-based or U.S. products that fall under U.S. ITAR export restrictions." [Data Fellow 1999c].

JCP Computer Services (United Kingdom)

JCP takes on U.S. products directly based on export controls [JCP 1999]:

> "Many companies are using or considering using implementations of these algorithms which originate in the US. The US government prohibits export of strong cryptographic tools, and, except under specific conditions, only permits the export of weak implementations. These 'crippled' cryptographic tools do not provide sufficient protection to allow Internet e-commerce and communications to proceed securely. In an amateur attack on a US export-strength cryptographic routine, the key was broken in 56 hours. And such times will decrease markedly as computer processing power continues to improve.
>
> "JCP has developed full strength implementations outside of the US using industry proven standard algorithms. JCP are the leading company outside the US producing high performance cryptographic tools in Java, which has become the Internet's standard programming language. The product provides a set of packages that implement specific cryptography algorithms for use within any Internet application."

SSH Communications Security (Finland)

SSH states on their web site [SSH 1999] that "The software from SSH is free from strict US export restrictions" as one of "six good reasons why SSH IPSEC Express is the best choise (sic)"; it goes on "IPSEC is supposed to be an international standard. However, because of export restrictions in different countries. (sic) SSH is one of the few to deliver full standards compliance and strong security virtually anywhere in the world."

RPK Security, Inc. (New Zealand, Switzerland, United Kingdom)

RPK advertises on its web site of its flagship RPK Encryptonite Engine [RPK 1999], "Developed outside the U.S., the RPK Encryptonite Engine is not subject to US government regulations. It is available with strong encryption worldwide, with dramatically better performance at significantly lower implementation cost compared with competing technologies." Reading further on its web site, one finds that "RPK's cryptographic research and product development is based in New Zealand, Switzerland and the U.K, with worldwide sales and marketing operations in San Francisco, CA."

6. STANDARDS AND THEIR INFLUENCE

6.1 Pervasiveness of Standards

From the material above, one can see that companies vie to have encryption products that meet certain accepted worldwide standards. If the products do not, they often will not interoperate successfully with other computer systems. This section highlights two important international standards efforts. Note the contribution of encryption expertise from all over the world to both.

6.1.1 IPsec

Today's widespread and pervasive use of the Internet has accentuated the need for security for the underlying Internet Protocol (IP). The IETF has developed the IP Security (IPsec) protocol as an integral element of internet security. IPsec is a proposed standard Internet protocol designed to provide cryptographic-based security, including authentication, integrity, and (optional) confidentiality services. While the use of IPsec is currently optional, its use will be mandatory for the next version of the Internet Protocol, IPv6 [IPsec].

As a result of the dramatic impact IPsec will have on improving the security of the Internet, there has been enormous interest in developing implementations of IPsec. This interest has extended throughout the entire world, due to the global nature of the Internet and need for cryptographic-based security. Many freely available and commercial implementations of IPsec are available or are under development. Ted Ts'o of MIT, co-chair of the IETF IPsec Working Group, maintains a list of companies implementing (or planning to implement) IPsec. The list currently cites implementations from 49 companies around the world. At least nine of the companies are from outside the U.S. There is also one effort, the KAME Project, being conducted by a combination of several Japanese companies (Fujitsu, Hitachi, IIJ Research Laboratory, NEC, Toshiba, and Yokogawa) [KAME 1999].

Another important aspect of IPsec is that it supports encrypted "tunnels", whereby an IP packet is completely encrypted as it travels from one point of a network to another. Encrypted tunnels are one of the primary means for establishing Virtual Private Networks, or VPNs, which emulate private networks over public, shared IP networks, such as the Internet.

IPsec is designed to be independent of any specific cryptographic algorithms; it can support several, but it will require one strong algorithm, Triple DES; the relatively weak DES will be permitted but not required. Specifications have also been developed for the use of the IDEA, BLOWFISH, RC5, and CAST strong cryptographic algorithms with long key lengths for IPsec [Stallings 1999].

6.1.2 Advanced Encryption Standard (AES)

In 1997, NIST solicited algorithms for the Advanced Encryption Standard (AES), to replace the Data Encryption Standard (DES) [FIPS PUB 46–2] as a government encryption standard. Individuals and companies from eleven different foreign countries proposed 10 out of the 15 candidate algorithms submitted to NIST [Smid 1998]:

Country	Candidate Algorithm	Submittor(s)
Australia	LOKI97	Lawrie Brown, Josef Pieprzyk, Jennifer Seberry
Belgium	RIJNDAEL	Joan Daemen, Vincent Rijmen
Canada	CAST–256	Entrust Technologies, Inc.
	DEAL	Outerbridge, Knudsen
Costa Rica	FROG	TecApro Internacional S.A.
France	DFC	Centre National pour la Recherche Scientifique (CNRS)
German	MAGENTA	Deutsche Telekom AG
Japan	E2	Nippon Telegraph and Telephone Corporation (NTT)
Korea	CRYPTON	Future Systems, Inc.
USA	HPC	Rich Schroeppel
	MARS	IBM
	RC6	RSA Laboratories
	SAFER+	Cylink Corporation
	TWOFISH	Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson
UK/Israel/Norway	SERPENT	Ross Anderson, Eli Biham, Lars Knudsen

"Of the five submissions likely to be chosen for the next round, about half will be from outside the U.S. It is very possible that the next U.S. government encryption standard will have been designed outside the U.S." [Schneier 1999].

7. CONCLUSIONS

Based on the research described above, we arrive at two conclusions:

1. Foreign development of cryptographic products is not only continuing but is expanding to additional countries.
2. Communications-related cryptography is experiencing high growth, especially in electronic mail, VPN, and IPsec products.

7.1 Foreign Development of Cryptography Continues to Grow

There are now 805 cryptography products produced in 35 countries outside the United States. In at least 67 countries, 512 foreign manufacturers and distributors are involved. In just three weeks, with limited resources, we identified 149 foreign cryptographic products new to market since the December 1997 TIS survey.

It is difficult to gauge how many additional products would be identified, given sufficient time and resources, but it is safe to anticipate that we would identify many more products from the countries within the database, and possibly several additional countries.

Development of cryptographic products in nations around the world is increasing. Moreover, as additional nations seize opportunities in e-commerce, nation-centric islands of competence develop, as do ultimately international markets. Often these islands of competence are developed by bright young entrepreneurs and computer scientists who have trained elsewhere (often the United States) and then play key roles in jump-starting their native countries' e-commerce. This fits nicely in the theory of technoglobalization, as espoused by Robert Reich, discussed more in Section 8.

7.2 Communications-Related Cryptography Leads Storage Cryptography

Within the 149 new products we discovered, communications-related products, as opposed to data storage encryption, were predominant. It appears that the efforts of the Internet Engineering Task Force (IETF) to provide standardized protocols for the Internet has facilitated the development of solutions and products to communications related problems. We conjecture that this and the expansion of e-commerce have resulted in a high growth of communications related cryptographic products such as those for electronic mail, VPNs, and IPsec.

Ipsec's support of encrypted tunnels will greatly improve security for private, enterprise-based networks. As the comfort level of users (and organizations) grows, and as the potential and actual gains of (consumer to business and business to business) e-commerce become apparent, there will be increased worldwide need for communications-related cryptography.

8. FUTURE RESEARCH

To date there have been only a few efforts to attempt to quantify the impact of regulatory measures on the international cryptographic market [Olbeter 1998, BSA 1998, CDT 1997]. The TIS survey and this effort to update the foreign products inventory of the database have been one of the few ways to quantitatively assess the state of the market over time. As noted in Section 7, we saw developments both in countries already producing cryptographic products and expansion into new countries that did not have cryptographic product development as of December 1997. We saw a number of firms become multinational.

In the face of continuing U.S. export controls on encryption products, technology, and services, some American companies have financed the creation or growth of foreign cryptographic firms. We have seen some U.S. companies (e.g., PGP, RSA, Sun) buy some foreign expertise, leaving it in place (rather than bringing the talent back to the United States). With this expertise offshore, the relatively stringent U.S. export controls for cryptographic products can be avoided, since products can be shipped from countries with less stringent controls. All of these facts indicate that both nations and companies see opportunities in this rapidly changing technological market, and it could be argued that globalization plays a major role in future growth for this market.

This is not a case of the technology slipping away from the United States. The technological expertise is already available in many places around the world. Indeed, we noted earlier that the majority of submissions for the Advanced Encryption Standard (AES) have been designed outside the United States. This may be simply an example of the general thesis of economists David Mowery and Nathan Rosenberg [Mowery 1989], who argue that, in general, foreign firms' technological sophistication has caught up with that of the United States in many cases. In those cases, they reason:

> "Since foreign firms now are more technologically sophisticated and technology is more internationally mobile, however, the competitive advantages that accrued in the past from basic research and a strong knowledge base have been eroded. Faster international transfer of new technologies is undercutting a major source of America's postwar superiority in high-technology markets." (p. 218)

Our empirical product data could be combined with economic measures and economic theories to better explain why we are seeing the observed growth in encryption products and companies around the world, and to examine the effects of Internet growth, e-commerce development, and regulatory actions on the international cryptographic market over time.

Porter [1990], for example, tests his theses by using quantitative measures from several nations, by industrial sector. His national economic profiles include primary goods, machinery, and specialty inputs and services data for each industrial sector. Given appropriate quantitative measures, similar work could be done for the international cryptography market.

As the global information-based economy continues to grow, and as the nature of industrial research and development continues to shift from nation-centric to international collaboration, we will continue to witness more rapid technological development and global economic growth. We should be able to put together previous economic work [Duysters 1996] with material already available on the information technology sector [Mowery 1996, Rosenberg [1992] and the data in this study to better understand the changes we are seeing in the global marketplace and thus be able to more easily adjust national laws for a global economy.

9. REFERENCES

[ABI/Inform]: ProQuest Direct, http://proquest.umi.com/pqdweb.

[Acey 1999]: Acey, Madeleine, TechWeb, CMPNet, in New York Times Technology, http://www.nytimes.com/techweb/
TW__Key__Escrow__Bill__Slammed__By__Parliament__Inquiry.html, 5/19/99.

[Adams 1997]: C. Adams, The CAST–128 Encryption Algorithm, RFC 2144, May 1997.

[Andrews 1997]: Andrews, Edmund L., "U.S. Restrictions of Exports Aid German Software Maker," New York Times, April 3, 1997.

[Argentina 1999]: Description of PGP and links to download it, in *Firma Digital y Documento Electrónico,* http://www.sfp.gov.ar/firma.html, downloaded May 27, 1999.

[Baker 1998]: Baker, S. and Hurst, P., *The Limits of Trust. Cryptography, Governments, and Electronic Commerce,* Kluwer Law International, 1998.

[Baltimore 1999a]: Baltimore Company Profile, http://www.baltimore.ie/corporate/profile.html.

[Baltimore 1999b]: WebSecure, http://www.baltimore.ie/products/websecure/index.html.

[Brokat 1998]: Brokat Offering Prospectus, http://www.brokat.com/int/ir/facts/annual__report.html.

[Brokat 1999a]: Brokat Company, http://www.brokat.com/int/company/index.html.

[Brokat 1999b]: Brokat Continues Success in Third Quarter, http://www.brokat.com/int/press/1999/pr19990519–01.html.

[Brokat 1999c]: Consulting Via Internet With X Agent From Brokat, http://www.brokat.com/int/press/1999/pr1 9990318–02.html.

[BSA 1998]: Business Software Alliance, The Cost of Government-Driven Key Escrow Encryption, 1998, http://www.bsa.org/ceoforum/pdfs/key__escrow.pdf

[CDT 1997]: Center for Democracy and Technology, The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption, a report by an ad hoc Group of Cryptographers and Computer Scientists, Washington, 1997.

[Check Point 1999a]: Check Point Corporate Information and News, http://www.checkpoint.com/corporate/index.html.

[Check Point 1999b]: Check Point Corporate Profile, http://www.checkpoint.com/corporate/corporate.html.

[Check Point 1999c]: Check Point Software Technologies Ltd Reports Financial Results for First Quarter 1999, http://www.checkpoint.com/press/1999/q1earnings041999.html.

[Commerce/NSA 1996]: *A Study of The International Market for Computer Software with Encryption,* Prepared by the U.S. Department of Commerce and the National Security Agency for the Interagency Working Group on Encryption and Telecommunications Policy, January 11, 1996.

[CPI 1999]: Non-U.S. Cryptographic Product Survey Call-for-Information, http://www.seas.gwu.edu/seas/institutes/cpi/cryptosurvey/call4info.html

[CSI 1997]: *Computer Security, Products Buyers Guide 1997,* Computer Security Institute, San Francisco, 1997.

[Cybernetica 1999a]: Cybernetica English Web Site, http://www.cyber.ee/infosecurity/products/privador/intro.html.

[Cybernetica 1999b]: Cybernetica Estonian Web site, http://www.cyber.ee/infoturve/tooted/privador/index.html.

[CRISIS 1996]: *Cryptography's Role in Securing the Information Society,* Kenneth W. Dam and Herbert S. Lin, Editors; Committee to Study National Cryptography Policy, National Research Council, 1996.

[Data Fellows 1999a]: Data Fellows Company Fact Sheet, http://www.datafellows.fi/df-info/.

[Data Fellows 1999b]: F-Secure Cryptography Products, http://www.datafellows. fi/f-secure/.

[Data Fellows 1999c]: F-Secure FileCrypto__On-the-fly encryption, http://www.datafellows.fi/f-secure/filecrypto/on-the-fly.htm.

[FIPS PUB 46–2]: National Institute of Standards and Technology. FIPS PUB 46–2: Data Encryption Standard. December 30, 1993.

[Dunlap 1999]: "All Tied Up: U.S. Trade Rules Hobble VARs, ISVs Alike Dealing With Encryption." by Charlotte Dunlap & Amy Rogers, Computer Reseller News, February 8, 1999.

[Duysters 1996]: Duysters, Geert. The Dynamics of Technical Innovation: The Evolution and Development of Information Technology. Cheltenham, U.K.: Edward Elgar.

[EDS 1996]: EDS, "When governments hamper encryption, they hamper commerce", advertisement, Washington Post, June 20, 1996.

[Entrust 1999]: Products: Entrust/SOLO, http://www.entrust.com/solo/index.htm.

[Ernst 1999]: Ernst & Young, Retail and Consumer Products: Key Technologies, http://www.ey.com/industry/consumer/retailit/key.asp, April 22, 1999.

[FirstSearch]: FirstSearch, http://gilligan.prod.oclc.org:3055/html/fs__areas.htm.

[Gale]: Gale Business Resources (integrated), http://www.galenet.com/servlet/GBR.

[Gibson 1998]: Paul Gibson, "The $237 billion conundrum", Electronic Business, Highlands Ranch, November 1998.

[GILC 1998]: Global Internet Liberty Campaign, "Online International Encryption Policy Survey, http://www.gilc.org/crypto/crypto-survey.html.

[Greenspan 1997]: Greenspan, Alan, Remarks at the Conference on Privacy in the Information Age, Salt Lake City, Utah, March 7, 1997, http://www.federalreserve.gov/boarddocs/speeches/19970307.htm

[Grossman 1999]: Wendy Grossman, Connected—Analysis: Encryption proves a slithery beast to control, Daily Telegraph (London), January 21, 1999.

[Hornstein 1999]: Testimony of Richard Hornstein before the Telecommunications, Trade and Consumer Protection Subcommittee of the Committee on Commerce, U.S. House of Representatives, Washington, DC, May 18, 1999.

[ICSA Survey]: ICSA Certified Cryptography Products ("Buyer's Guide"), list is at http://www.icSa.net/services/consortia/cryptography/certified__products.shtml.

[IKE]: Harkins, D., and D. Carrel, D., The Internet Key Exchange (IKE), RFC 2409, November 1998.

[IPSEC]: S. Kent and R. Atkinson, Security Architecture for the Internet Protocol, RFC 2401, November 1998.

[IPSECIPM]: Ted T'so, IPSEC/ISAKMP Company List, Companies which are Implementing (or Planning to Implement) IPSEC/ISAKMP, http://web.mit.edu/tytso/www/ipsec/.

[IPSECWG]: IPsec WG Charter, http://www.ietf.org/html.charters/ipsec-charter.html.

[JCP 1999]: JCP Computer Services, http://wwwjcp.co.uk/secProduct/security__cdk__index.htm.

[KAME 1999]: KAME Project, http://www.kame.net/.

[Koops 1999a]: Koops, B-J, Crypto Law Survey, http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm.

[Koops 1999b]: Koops, B-J, *The Crypto Controversy: A Key Conflict in the Information Society,* Kluwer Law International, The Hague, 1999.

[Lai 1990]: Lai, X., and Massey, J., A Proposal for a New Block Encryption Standard, Proceedings EUROCRYPT '90, Springer Verlag, 1990.

[Lai 1991]: Lai, X., and Massey, J., Markov Ciphers and Differential Cryptanalysis, Proceedings of EUROCRYPT '91, Springer-Verlag, 1991.

[Lexis Nexis]: Lexis-Nexis, http:/www.lexis-nexis.com.

[Matsui 1996]: Mitsuru Matsui, New Block Encryption Algorithm MISTY, Mitsubishi Electric Corp., 1996.

[MISTY]: MISTY__Mitsubishi Electronic's Encryption Algorithm, http://www.mitsubishi.com/ghp__japan/misty/200misty.htm.

[Mowery 1989]: Mowery, David C. and Nathan Rosenberg. Technology and the Pursuit of Economic Growth. Cambridge UK: Cambridge University Press, 1989.

[Mowery 1996]: Mowery, David C. (ed.). The International Computer Software Industry: A Comparative Study of Industry Evolution and Structure. New York: Oxford University Press.

[Olbeter 1998]: Olbeter, Erik R. and Christopher Hamilton, Finding the Key: Reconciling National and Economic Security Interests in Cryptography Policy, Economic Strategy Institute, Washington, DC, March 1998.

[PECSENC 1998]: Report of the president's Export Council Subcommittee on Encryption Working Group on International Affairs, September 1998, http://209.122.145.150/PresidentsExportCouncil/PECSENC/iwgfind.htm.

[Porter 1990]: Porter, Michael E., *The Competitive Advantage of Nations,* New York: The Free Press, 1990.

[Randata 1999]: Media Release, "Boost For Smart Aussie Company: SNS The First To Be Granted U.S. Export License For High Security Cryptography," Sept. 7, 1998. http://www.randata.com.au/infblx.htm.

[Reich 1990]: Robert B. Reich, "Does Corporate Nationality Matter?", Issues in Science and Technology, Winter 1990–91, pp. 40–44.

[Reinsch 1999]: Reinsch, William A., Testimony before the House Committee on Commerce, Subcommittee on Telecommunications, Trade and Consumer Protection, May 25, 1999.

[Rivest 1978]: R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", *Communications of the ACM, February 1978,* Volume 21, Number 2, pp. 120–126.

[Rivest 1996]: [Rivest 1996] R. Rivest and R. Baldwin, The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms, RFC 2040, October 1996.

[Rosenberg 1992]: Rosenberg, Nathan, Ralph Landau, and David C. Mowery (eds). Technology and the Wealth of Nations. Stanford, Calif.: Stanford University Press.

[RPK 1999]: RPK Security, http:/www.rpk.com/.

[RSA 1999]: "RSA Provides Security Solutions to Worldwide Markets Through New Operation in Australia", January 6, 1999 press release, http://www.aus.rsa.com/pressbox/990106-1.html.

[Schneier 1993]: Schneier, B., Description of a New Variable-Length Key, 64-bit Block Cipher (Blowfish), Proceedings of Workshop on Fast Software Encryption, Springer Verlag, 1993.

[Schneier 1994]: Schneier, B., The Blowfish Encryption Algorithm, Dr. Dobb's Journal, April 1994.

[Schneier 1995]: Schneier, B., *Applied Cryptography: Protocols, Algorithms, and Source Code in C,* 2nd ed., Wiley, 1995.

[Schneier 1999]: Bruce Schneier, The Internationalization of Cryptography, CRYPTOGRAM Newsletter, May 15, 1999, http://www.counterpane.com/crypto-gram-9905.html.

[Smid 1998]: Smid, M., and M. Dworkin, Special Report on the First AES Conference, presented at Crypto '98 Conference, August 1998, http://csrc.nist.gov/encryption/aes/round1/crypto98.pdf.

[Sophos 1999]: Sophos Company Info, http://www.sophos.com/companyinfo/profile/.

[SSH 1999]: 6 Good Reasons Why SSH IPSEC Express is the Best Choice, http://www.ipsec.com/6reasons.html.

[Stallings 1999]: William Stallings, *Cryptography and Network Security. Pinciples and Practice,* Second Edition, Prentice Hall, 1999.

[Thayer 1997]: Rodney Thayer, "Bulletproof IP" in Data Communications, November 21, 1997, http://data.com/tutorials/bullet.html.

[TIS 1997]: Worldwide Survey of Cryptographic Products, http://www.nai.com/products/security/tis__research/crypto/crypt__surv.asp, December 1997.

[United Nations 1986]: U.N. International Trade Statistics Yearbook, 1986. New York: United Nations.

[U.S. DoC 1996]: U.S. Department of Commerce Press Release, "Department of Commerce Releases Study on the International Market for Encryption Software", January 11, 1996.

[Utimaco 1999a]: Utimaco Safeware AG Facts and Figures, http://www.utimaco.de/english/index1.htm.

[Utimaco 1999b] SafeGuard VPN Product Description, http://www.utimaco.com/english/products/sgvpn__e.htm.

[Walker 1993] Testimony of Stephen Walker before the U.S. House of Representatives Foreign Affairs Subcommittee on Economic Policy, Trade and Environment, October 12, 1993.

[Walker 1994] Testimony of Stephen Walker before the U.S. Senate Judiciary Subcommittee on Technology and the Law, Hearing on the Administration's "Clipper Chip" Key Escrow Encryption Program, May 13, 1994.

APPENDICES

A. CALL FOR INFORMATION

Please forward this message to others who are interested on the topic. A WWW-version of this message can be found at http://www.seas.gwu Xedu/seas/institutes/cpi/cryptosurveylcall4info.html

Non-U.S. Cryptographic Product Survey Call for Information

The George Washington University and NAI Labs, The Security Research Division of Network Associates (formerly the research division of Trusted Information Systems) are conducting a survey to identify cryptographic products manufactured outside the United States and are examining product specifications to assess their functionality and security.

We are soliciting input from those with knowledge of cryptographic products through the use of this survey form. If you know of cryptographic products that are manufactured in countries other than the United States, please complete this form and submit it to the Cyberspace Policy Institute (CPI) NO LATER THAN TUESDAY MAY 18, 1999. You may submit this form via email to cpiWseas.gwu.edu or fax at (202) 994–5505 in Washington D.C.

In addition, we ask you to send or post this survey to anyone or place that would have knowledge of cryptographic products. Inquiries about this survey may be made to the Cyberspace Policy Institute at cpi@seas.gwu.edu or (202) 994–5512. This survey may also be found on the CPI Web site at http://www.seas.gwu.edu/seas/institutes/cpi.

Your cooperation is greatly appreciated.

Professor Lance J. Hoffman, The George Washington University David Balenson, NAI Labs, The Security Research Division of Network Associates

NON-U.S. CRYPTOGRAPHIC PRODUCT SURVEY

DATE:
COMPLETED BY:
Your Name:
Phone:

E-mail:

NAME AND ADDRESS OF MANUFACTURER

Name:
Address:
City:
State:
Zip Code:
Country:
URL:

MANUFACTURER CONTACT INFORMATION

Name:
Phone:
E-mail:
Title:
FAX:
800#:

PRODUCT DESCRIPTION

Name (including model and version information):

Product-specific URL:

Is it software-only, hardware-only, or a software/hardware combination?

What does it encrypt (e.g., disk, file, communications, FAX, voice, magnetic tape, electronic mail)?

If embedded software or hardware, what platforms does it support (e.g., PC, Mac, UNIX workstation, IBM mainframe), else if standalone hardware, what interfaces does it support (RS–232, telephone, V.24, V.35)?

If software, is it in the form of a kit or as an end-user program, else if hardware, what is the embodiment (e.g., chip, board, PCMCIA card, smart card, box, phone)?

What algorithms does it employ for data encryption (including proprietary algorithms and key length)?

If applicable, what algorithms does it employ for key management (including proprietary algorithms and key length)?

If applicable, what algorithms does it employ for data authentication (including proprietary algorithms)?

How is the product sold or distributed (e.g., store front, mail order, telephone order, World Wide Web, anonymous ftp over the Internet)?

If applicable, what is the quantity one purchase price?

(Optional) Approximate number of units sold or distributed?

(Optional) Approximate date product was first available?

Please provide a list of the names and relationships of any associated companies (e.g., parent company, sister company, distributors). Include full address and contact name, title, phone, FAX, and e-mail address.Other information:

Please Provide a Copy of Any Relevant Product Literature.

Send completed forms and product literature via e-mail to cpi@seas.gwu.edu or via fax to the Cyberspace Policy Institute at 202–994–5505 in Washington D.C.

Thank You!

This survey is part of an ongoing worldwide study of cryptographic products started in April 1994 by Trusted Information Systems and Dr. Lance J. Hoffman of the George Washington University. The December 1997 summary results of the survey are available on the World Wide Web at http://www.nai.com/products/security/tis__research/cryptolCrypt__surv.asp.

B. SUMMARY LISTING OF FOREIGN CRYPTOGRAPHIC PRODUCTS

The following table is a summary listing of the foreign products currently contained in the cryptographic product database. We cannot guarantee the accuracy and completeness of this information. In many cases, products may support additional platforms or interfaces, encrypt additional types of information, include additional embodiments, or support additional encryption algorithms. Additional information will be available on the NAI Labs Crypto Products Survey Web page at http://www.nai.com/products/security/tis__research/crypto/crypt__surv.asp.

COUNTRY	COMPANY	PRODUCT	PLATFORMS/ INTERAFCES	TYPE	ENCRYPTS	EMBODIMENT	ENC ALG
ARGENTINA	DataCrypt	Software implementation of Criptography	DOS	SW	GENERAL	PGM	DES
ARGENTINA	Newnet S.A.	DSD 9612 Data Security Device	TTL	HW	GENERAL	CHIP	DES
AUSTRALIA	Andrei Souleimanian	Xbact		SW	FILE	PGM	PROP
AUSTRALIA	Banksia Technology Pty. Ltd	Citadel	V.34	HW	COMMS	BOX	DES
AUSTRALIA	Banksia Technology Pty. Ltd.	Pro 144	V.32	HW	COMMS	BOX	DES
AUSTRALIA	Banksia Technology Pty. Ltd	Pro 34	V.34	HW	COMMS	BOX	DES
AUSTRALIA	Banksia Technology Pty. Ltd	Procard 34	V.34	HW	COMMS	PCMCIA	DES
AUSTRALIA	Carbon Based Software	CryptStream	OS2	SW	FILE	PGM	DES
AUSTRALIA	Carbon Based Software	Zipstream Secure	OS2	SW	FILE	PGM	DES
AUSTRALIA	Cipher Research Laboratories	??					
AUSTRALIA	Cryptsoft Pty Ltd.	SSLeay	DOS	SW	SSL	PGM	RSA
AUSTRALIA	Cryptsoft Pty Ltd.	SSLftp	DOS	SW	FTP	PGM	DES
AUSTRALIA	Cybanim Pty Ltd	DES32 v1.02	PC	SW	GENERAL	KIT	DES
AUSTRALIA	Cybanim Pty Ltd.	DESF v1.4	PC	SW	GENERAL	PGM	DES
AUSTRALIA	Cybanim Pty Ltd.	LUC 2.03	PC	SW	GENERAL	PGM	LUC
AUSTRALIA	Cybanim Pty Ltd	SIFR v2.0	PC	SW	GENERAL	PGM	RSA
AUSTRALIA	DataCrypt	LetterCrypt	PC	SW	COMMS	PGM	
AUSTRALIA	DataCrypt	NoteCrypt	PC	SW	FILE	PGM	
AUSTRALIA	DataCrypt	PassCrypt	DOS	SW	FILE	PGM	
AUSTRALIA	Eracom Pty Ltd	CF 7000 Intelligent Encryption Adaptor	PCI	HW	GENERAL	BOARD	DES
AUSTRALIA	Eracom Pty Ltd	CP500 Slave Encryption Adaptor	PCI	HW	GENERAL	BOARD	DES
AUSTRALIA	Eracom Pty Ltd.	CPROV	SOLARIS	HW	GENERAL	BOARD	DES
AUSTRALIA	Eracom Pty Ltd.	CSA 7000 PCI Hardware Crypto Adaptor	PCI	HW	GENERAL	BOARD	DES
AUSTRALIA	Eracom Pty Ltd	Encryption Services API	OS2	SW	GENERAL	KIT	DES
AUSTRALIA	Eracom Pty Ltd.	ERA 2007 Line Encryptor	RS232	HW	COMMS	BOX	DES
AUSTRALIA	Eracom Pty Ltd.	ERA 4007 Line Encryptor	V.24	HW	COMMS	BOX	DES
AUSTRALIA	Eracom Pty Ltd.	JPROV	SOLARIS	HW	GENERAL	BOARD	DES
AUSTRALIA	Eracom Pty Ltd	MCE Slave Encryption Adaptor	PC	HW	GENERAL	BOARD	DES
AUSTRALIA	Eracom Pty Ltd.	PC Vault	DOS	SW	DISK	PGM	DES
AUSTRALIA	Eracom Pty Ltd	PCASM Intelligent Encryption Adaptor	ISA	HW	GENERAL	BOARD	DES
AUSTRALIA	Eracom Pty Ltd	PCE Slave Encryption Adaptor	ISA	HW	GENERAL	BOARD	DES
AUSTRALIA	Eracom Pty Ltd.	ProtectSNA	ERACOM BOARDS	SW/HW	COMMS	BOARD	DES
AUSTRALIA	Eracom Pty Ltd	RSA API	OS2	SW	GENERAL	PGM	RSA
AUSTRALIA	Eracom Pty Ltd.	SECLink	X.25	HW	COMMS	BOARD	DES
AUSTRALIA	Eracom Pty Ltd	SECPac	X.25	HW	COMMS	BOARD	DES
AUSTRALIA	Eracom Pty Ltd	Series 90 Eracom Security Module (ESM)	RS232	HW	COMMS	BOX	DES
AUSTRALIA	Enc Young	CryptL99	ANY	SW	GENERAL	PGM	DES
AUSTRALIA	Enc Young	fcrypt	ANY	SW	FILE	PGM	DES
AUSTRALIA	Enc Young	libdes	ANY	SW	GENERAL	KIT	DES
AUSTRALIA	Meralock	Kinetic Access		SW	FILE		
AUSTRALIA	Mosaic Industries	Touch Lock	WIN95	SW	DISK	PGM	PROP
AUSTRALIA	Mosaic Industries	Touch Net II		SW/HW	FILE		
AUSTRALIA	NetSafe	EXE Guardian	ANY	SW	PROGRAMS	KIT	DES
AUSTRALIA	News Datacom	N-Sure Access 1000	WK	HW	COMMS	BOARD	DES
AUSTRALIA	NexSol	Ntrust	WIN	SW	FILE	KIT	
AUSTRALIA	Nick Payne	Cryptext	WIN95	SW	FILE	PGM	RC4
AUSTRALIA	Randata	Megacrypt High Speed Data Encryptor	RS422/V.11	HW			PROP
AUSTRALIA	Robust Software	Block-It					
AUSTRALIA	RSA Data Security Australia	RSA BSAFE SSL-C v1.0	WIN32	SW	SSL	KIT	DES
AUSTRALIA	Secure Network Solutions	FAXSAFE	telephone	HW	VOICE	BOX	PROP
AUSTRALIA	Secure Network Solutions	GSA 1000 Duplex Mini Scrambler	RADIO	HW	VOICE	BOARD	
AUSTRALIA	Secure Network Solutions	GSA 1300	RADIO	HW	VOICE	BOARD	PROP
AUSTRALIA	Secure Network Solutions	Guardian-E Data Encryptor	RS232	HW	COMMS	BOX	DES
AUSTRALIA	Secure Network Solutions	Guardian-EM Encryptor Modem	RS232	HW	COMMS	BOX	DES
AUSTRALIA	Secure Network Solutions	Guardian-EMP Data Encryptor	RS232	HW	COMMS	BOX	DES
AUSTRALIA	Secure Network Solutions	Guardian-EP Data Encryptor	RS232	HW	COMMS	BOX	DES
AUSTRALIA	Secure Network Solutions	Megacrypt High Speed Data Encryptor	RS422/V.11	HW	COMMS	BOX	PROP

AUSTRALIA	Secure Network Solutions	RD185 Fax	telephone	HW	FAX	BOX	PROP
AUSTRALIA	Secure Network Solutions	RD187 Data Encryptor	RS232	HW	COMMS	BOX	DES
AUSTRALIA	Secure Network Solutions	Secure Management Systems(SMS)	ETHERNET	SW/HW	COMMS	PGM	3DES
AUSTRALIA	Secure Network Solutions	SecureLine	TELEPHONE	HW	FAX	BOX	DES
AUSTRALIA	Secure Network Solutions	SecureNET Data Encryptor	X.25	HW	COMMS	BOX	DES
AUSTRALIA	Secure Network Solutions	SecureNET HSP	ETHERNET	HW	COMMS	BOX	DES
AUSTRALIA	Secure Network Solutions	SecurLAN Network Encryption Unit - Router (NEU-RT)		HW	COMMS	BOX	DES
AUSTRALIA	Secure Network Solutions	SecurLink Data Encryptor	RS232	HW	COMMS	BOX	DES
AUSTRALIA	Secure Network Solutions	SecurPAC EM Encryptor Modem	V.24	HW	COMMS	BOX	DES
AUSTRALIA	Secure Network Solutions	SecurPAC IEM	ETHERNET	HW	COMMS	PCMCIA	DES
AUSTRALIA	Secure Network Solutions	SecurPac PEM Data Encryptor	X.25	HW	COMMS	BOX	DES
AUSTRALIA	Security Domain Pty Ltd	Secure Attache	WIN	SW	FILE	PGM	DES
AUSTRALIA	TRAC Systems	??					
AUSTRALIA	Tracom	??					
AUSTRIA	Eshelbeck, Steiner, Beilelmair	Coded Drag	WIN95	SW	FILE	PGM	DES
AUSTRIA	IAIK, TU Graz	IAIK JCE (Java Cryptographic Extension)	JAVA	SW	GENERAL	KIT	DES
AUSTRIA	Mils Electronik	System 700	PC			PGM	
AUSTRIA	Mils Elektronik			HW	VOICE	PHONE	
AUSTRIA	Mils Elektronik	Fax Encryptor		HW	FAX	BOX	
AUSTRIA	Siemens AG Austria	Document Security Service (DSS) Version 2	WIN	SW	FILE	KIT	DES
AUSTRIA	University of Linz	Coded Drag	WIN95	SW	FILE	PGM	DES
BELGIUM	CNET	RSA chip	TTL	HW	GENERAL	CHIP	RSA
BELGIUM	RSA Ran Data Europe	MARTLET					
BELGIUM	Highware, Inc.	FileCrypt	MAC	SW	EMAIL	PGM	
BELGIUM	Highware, Inc.	Fileguard 3.0	MAC	SW	FILE	PGM	DES
BELGIUM	Lintel Security	CRY12C102 DES Chip		HW	GENERAL	CHIP	3DES
BELGIUM	Lintel Security	PC DES/RSA Card	PC	SW/HW	COMMS	PCMCIA	DES
BELGIUM	Lintel Security	POR 512 RSA Chip	TTL	HW	GENERAL	CHIP	RSA
BELGIUM	UTI-MACO Belgium	CryptMail	ANY	SW	EDI	PGM	DES
BELGIUM	Vector	??					
CANADA	Adam Beient	ABI-Coder 2.0	WIN32	SW	FILE	PGM	PROP
CANADA	Atlantic Systems Group (ASG)	TumStyle Firewall System (TFS)	UNIX	SW	COMMS	PGM	DES
CANADA	Authentex/NovaStor	DataSafe	WIN	SW	FILE	PGM	BLOWFISH
CANADA	Authentex/NovaStor	QuickSafe	WIN	SW	FILE	PGM	BLOWFISH
CANADA	Authentex/NovaStor	Security Suite	WIN32	SW	FILE	PGM	BLOWFISH
CANADA	Certicom	CardSecrets CS 1000	ANY	HW	COMMS	PCMCIA	DES
CANADA	Certicom	Elliptic Curve Toolkit (Beta Version)	DOS	SW	GENERAL	KIT	DES
CANADA	Certicom	FaxSecrets FS 1000	RJ-11	HW	FAX	BOX	DES
CANADA	Certicom	FS 3000		HW	FAX	BOX	
CANADA	Certicom	MOBIUS Integrated Security Solutions	ANY	SW	GENERAL	KIT	DES
CANADA	Certicom	Security Builder Crypto Toolkit		SW		KIT	DES
CANADA	Certicom	TaxSecrets	PC	SW	FILE	PGM	DES
CANADA	Certicom	TradeSecrets TS 2000	PC	HW	COMMS	BOARD	DES
CANADA	Chrysalis ITS	LUNA 2	WIN/NT	SW/HW	COMMS	PCMCIA	DES
CANADA	Chrysalis ITS	LUNA CA	WIN/NT	SW/HW	KEYS	PCMCIA	DES
CANADA	Chrysalis ITS	LUNA ToolKit	WIN/NT	SW/HW	COMMS	PCMCIA	DES
CANADA	Chrysalis ITS	LUNA VPN	WIN/NT	SW/HW	VPN	BOARD	DES
CANADA	Compression Technologies, Inc.	CTI WARP II	RS232	HW	COMMS	BOX	PROP
CANADA	Compression Technologies, Inc.	CTI WARP III	RS232	HW	COMMS	BOX	PROP
CANADA	Compression Technologies, Inc.	WARP IV Frame Master	V.35	SW/HW	COMMS	KIT	
CANADA	CRYPTOCard Corporation	SB-1 Electronic Diskette Token	PC	HW	DISK	DISK	PROP
CANADA	Earthworks Communications	??		SW			
CANADA	Entrust Technologies	Entrust File Toolkit		SW	COMMS	KIT	DES
CANADA	Entrust Technologies	Entrust Lite	WIN	SW	FILE	PGM	DES
CANADA	Entrust Technologies	Entrust/Client	MAC	SW	FILE	PGM	DES
CANADA	Entrust Technologies	Entrust/Direc	WIN	SW	COMMS	PGM	RSA
CANADA	Entrust Technologies	Entrust/ICE 4.0	WIN/NT	SW	FILE	PGM	DES
CANADA	Entrust Technologies	Entrust/Manager	MAC	SW	COMMS	PGM	PROP
CANADA	Entrust Technologies	Entrust/Session Toolkit	MAC	SW	COMMS	KIT	DES
CANADA	Entrust Technologies	Entrust/Solo	WIN95	SW	DISK	PGM	CAST
CANADA	Freestyle Software, Inc.	Avalanche Java Cryptographic Toolkit		SW	GENERAL	KIT	DES
CANADA	Gandalf	Gandalf/LZA Plus	PC	SW	COMMS	PGM	PROP
CANADA	Ilex Systems Inc.	Securafile	WIN	SW	EMAIL	PGM	DES
CANADA	Inforon Technologies, Inc.	NETSEC		SW			
CANADA	Isolation Systems	Infocrypt Desktop	WIN95	SW	COMMS	PGM	DES
CANADA	Isolation Systems	Infocrypt Enterprise	ENET	HW	COMMS	BOX	DES
CANADA	Isolation Systems	Infocrypt Extreme PCI	DOS	HW	COMMS	BOARD	DES
CANADA	Isolation Systems	Infocrypt Server	WIN/NT	SW	COMMS	PGM	DES
CANADA	Isolation Systems	Infocrypt Solo	WIN95	SW	VPN	PGM	DES
CANADA	Isolation Systems	ISAC 1100	PC	HW	COMMS	BOARD	DES
CANADA	Isolation Systems	ISAC 1500	TOSHIBA	SW/HW	COMMS	BOARD	DES
CANADA	Isolation Systems	ISAC 2200	PC	HW	COMMS	BOARD	DES
CANADA	Isolation Systems	ISAC 2400	PC	HW	COMMS	BOARD	DES
CANADA	Isolation Systems	ISAC 2500	PC	HW	COMMS	BOARD	DES
CANADA	Isolation Systems	ISAC 3200	PC	HW	COMMS	BOARD	DES
CANADA	Isolation Systems	ISAC 3500	PC	HW	COMMS	BOARD	DES
CANADA	Isolation Systems	ISAC 4200	MAC	HW	COMMS	BOARD	DES
CANADA	Isolation Systems	ISBR		HW	COMMS		
CANADA	Isolation Systems	ISE 2100	PC	HW	COMMS	BOARD	DES
CANADA	Isolation Systems	ISFE Frame Relay	NETWORK	SW/HW	COMMS	PGM	DES
CANADA	Isolation Systems	ISPE/M		HW	COMMS		DES
CANADA	Isolation Systems	ISPE/R (Isolation System Packet Encryptor/Router)	NETWORK	SW/HW	COMMS	BOARD	DES
CANADA	Isolation Systems	ISPE/SA (Standalone Version)	NETWORK	HW	COMMS		DES
CANADA	Isolation Systems	ISTM (Isolation System Table Management)	NETWORK				
CANADA	Isolation Systems	ISXE/M	X.25				
CANADA	Kyberpass Corporation	Kyberpass	WIN	SW	COMMS	PGM	DES

CANADA	Micro Tempus, Inc.	Tempus-CLIP	DOS	SW/HW		PGM	
CANADA	Milkyway Networks Corporation	Black Hole	ANY	SW	COMMS	PGM	
CANADA	MPR Teltech	??			SATELLITE		
CANADA	Northern Telecom Canada Ltd. (Data Comm. Products)	Packet Data Security Overlay (PDSO)	ANY	HW	COMMS	BOX	DES
CANADA	Northern Telecom Secure Networks	DMS NTX Switch (Cellular) CDPD					
CANADA	Octothorp Industries	Canine Mail	WIN32	SW	EMAIL	PGM	BLOWFISH
CANADA	Okiok Data	Data Encryption Board (DEB)	PC	HW	FILE	BOARD	DES
CANADA	Okiok Data	FileSafe Light	WIN	SW	FILE	PGM	
CANADA	Okiok Data	RAC/M IX IPC	PCI	HW	EDI	SMART CARD	DES
CANADA	Okiok Data	RAC/M Open Cryptographic Server	OS2	HW	EDI	PC	DES
CANADA	Okiok Data	Secure Server for Netware	NOVELL	SW/HW	FILE	WK	DES
CANADA	Queen's University	RSA chip		HW		CHIP	RSA
CANADA	Scientific Atlantic	??			Pay TV		PROP
CANADA	Secure Computing Corporation	BorderWare Firewall Server	PC	SW/HW	COMMS	KIT	DES
CANADA	Secure ISDN Terminals	Rex					
CANADA	Secured Communications Inc. (SCI)	Session Key	PC	HW	FILE	PCMCIA	DES
CANADA	Sierra Wireless	CDPD (Cellular Digital Packet Data)	V.32		EMAIL		RSA
CANADA	Sierra Wireless	PocketPlus	WIN	HW		BOX	CDPD
CANADA	Silanis Technology	Approvelt CAD	WIN	SW	FILE	PGM	DES
CANADA	Silanis Technology	Approvelt Desktop	WIN	SW	FILE	PGM	PROP
CANADA	Silanis Technology	Approvelt Toolkit	WIN	SW	GENERAL	KIT	DES
CANADA	The Enigma Group	ENIGMA-7 Encryption	WIN	SW	FILE	PGM	PROP
CANADA	TimeStep Corporation	PERMIT 1010 PC LAN Security Module	pc	SW/HW	COMMS	PGM	DES
CANADA	TimeStep Corporation	PERMIT 1011 PC LAN Security ISA Card	pc	SW/HW	COMMS	PGM	DES
CANADA	TimeStep Corporation	PERMIT 1012 PC LAN Security PCI Card	pc	SW/HW	COMMS	PGM	DES
CANADA	TimeStep Corporation	PERMIT 1013 PC LAN Security MCA Card	pc	SW/HW	COMMS	PGM	DES
CANADA	TimeStep Corporation	PERMIT 1060 Secure Ethernet Bridge	WIN	SW/HW	COMMS	BOX	3DES
CANADA	TimeStep Corporation	PERMIT 2010 PC LAN Security Module	PC	SW/HW	COMMS	BOARD	DES
CANADA	TimeStep Corporation	PERMIT 2018 PC Remote Security		SW	COMMS	PGM	DES
CANADA	TimeStep Corporation	PERMIT 3010	PC	SW/HW	DISK	BOARD	DES
CANADA	TimeStep Corporation	PERMIT 9010 SNMS	PC	SW/HW	IPSEC		DES
CANADA	TimeStep Corporation	PERMIT 9300	pc	SW/HW	COMMS	PGM	
CANADA	TimeStep Corporation	PERMIT SToken	PC	HW	GENERAL	PCMCIA	
CANADA	TimeStep Corporation	PERMIT Security Gateway	NETWORK	HW	COMMS	BOX	
CANADA	TimeStep Corporation	PERMIT Security MicroGate	ENET	HW	COMMS	BOX	
CANADA	TimeStep Corporation	PERMIT SVPN		HW	VPN		
CANADA	Tundra Semiconductor Corp.	CA20C03A	TTL	HW	GENERAL	CHIP	DES
CANADA	Tundra Semiconductor Corp	CA20C03A/W DES Encryption Processor					DES
CANADA	Tundra Semiconductor Corp.	CA20C03W		HW	GENERAL	CHIP	DES
CANADA	Tundra Semiconductor Corp.	CA95C68118/09	TTL	HW	GENERAL	CHIP	DES
CANADA	Tundra Semiconductor Corp.	NM830	PC	SW/HW	FILE	PGM	
CANADA	Tundra Semiconductor Corp.	Permit LAN Encryption modules for LAN adapters					
CANADA	Tundra Semiconductor Corp.	Transmission Access Platform (TAP)	RS232	HW		BOX	DES
CANADA	Xcert International Inc.	Sentry CA	WIN/NT	SW/HW	KEYS		RSA
CANADA	Xcert International Inc.	Sentry RA	WIN/NT	SW/HW	KEYS		RSA
CANADA	Zoomit Corporation	Remote Link Plus	PC	SW	COMMS		RSA
CZECH REPUBLIC	Alwil Software	Access Control SUPervisor	DOS	SW	FILE	PGM	
CZECH REPUBLIC	Alwil Software	Fort Knox		SW	DISK	PGM	
CZECH REPUBLIC	Decros spol. s r.o.	Protect95	WIN95	SW	FILE	PGM	PROP
CZECH REPUBLIC	Decros spol. s r.o.	ProtectNT	WIN/NT	SW	FILE	PGM	PROP
CZECH REPUBLIC	Decros spol. s r.o.	Security Card		HW			
DENMARK	Aarhus University, Computer Science Department	VICTOR	TTL	HW	GENERAL	CHIP	RSA
DENMARK	CryptoMathic A/S	6303 SIS	6303MP	SW	GENERAL	PGM	SIS
DENMARK	CryptoMathic A/S	8051 DES	INTEL 8031	SW	GENERAL	PGM	DES
DENMARK	CryptoMathic A/S	DES for IBM/370	MF	SW		KIT	DES
DENMARK	CryptoMathic A/S	DES Kernel	PC	SW	GENERAL	KIT	DES
DENMARK	CryptoMathic A/S	DES Security Mechanisms	PC	SW	GENERAL	KIT	DES
DENMARK	CryptoMathic A/S	DSP 56000 DES	DSP56000/1	SW	GENERAL	PGM	DES
DENMARK	CryptoMathic A/S	DSP 56000 RSA	DSP56000/1	SW	GENERAL	PGM	RSA
DENMARK	CryptoMathic A/S	F2F (File-to-File)	PC	SW	FILE	PGM	DES
DENMARK	CryptoMathic A/S	Multiprecision Kernel	PC	SW	GENERAL	KIT	RSA
DENMARK	CryptoMathic A/S	PrimeDrink Java Toolbox	JAVA	SW	GENERAL	KIT	DES
DENMARK	CryptoMathic A/S	PrimeInk C Toolbox	C CODE	SW	GENERAL	KIT	DES
DENMARK	CryptoMathic A/S	RSA Security Mechanisms	PC	SW	GENERAL	KIT	RSA
DENMARK	CryptoMathic A/S	Security API		SW		KIT	DES
DENMARK	GN Datacom	safeMatic Security Module	ANY	HW	COMMS	BOX	DES
DENMARK	Intellitech Omniware	iCrypt 3.2	WIN95	SW	FILE	PGM	DES
DENMARK	Kommunedata	EDI-SAFE	PC	HW	COMMS	CHIP	
DENMARK	LSI Logic/Dataco AS	Dataco LSA4043 2030025402	PC	HW	GENERAL	CHIP	DES
DENMARK	LSI Logic/Dataco AS	Dataco LSA4043 2030025402	TTL	HW	GENERAL	CHIP	DES
DENMARK	Telesec	TelesecC	ANY	SW	EDI	KIT	DES
ESTONIA	Cybernetica	Privador SVPN	ETHERNET	SW/HW	IPSEC	BOX	DES
ESTONIA	Cybernetica	Secure Socket Agent	WIN95	SW	COMMS	PGM	3DES
FINLAND	Antti Louko	AloDES	ANY	SW	GENERAL	PGM	DES
FINLAND	Datafellows Ltd.	F-Secure Commerce	WIN	SW	COMMS	PGM	DES
FINLAND	Datafellows Ltd.	F-Secure Desktop	WIN	SW	FILE	PGM	BLOWFISH
FINLAND	Datafellows Ltd.	F-Secure FileCrypto	WIN/NT	SW	FILE	PGM	3DES
FINLAND	Datafellows Ltd	F-Secure SSH Client	MAC	SW	COMMS	PGM	

FINLAND	Datafellows Ltd.	F-Secure SSH Server	UNIX	SW	COMMS	PGM	3DES
FINLAND	Datafellows Ltd.	F-Secure SSH Tunnel&Terminal	MAC	SW	COMMS	PGM	RSA
FINLAND	Datafellows Ltd.	F-Secure Virtual Private Network	PC	SW	VPN	PGM	3DES
FINLAND	Datafellows Ltd.	F-Secure VPN+	WIN95	SW	IPSEC	PGM	DES
FINLAND	Jetico, Inc.	BestCrypt NP	WIN95	SW	FILE	PGM	BLOWFISH
FINLAND	Jetico, Inc.	BestCrypt Lite	WIN	SW	FILE	PGM	DES
FINLAND	Jetico, Inc.	BestCrypt+	WIN	SW/HW	FILE	PGM	GOST 28147-89
FINLAND	Jetico, Inc.	LS06C20		HW		CHIP	GOST28147
FINLAND	SSH Communications Security	SSH	MAC	SW	COMMS	PGM	ELGAMAL
FINLAND	SSH Communications Security	SSH IPSec Express Toolkit	ANY	SW	IPSEC	KIT	3DES
FINLAND	SSH Communications Security	SSH ISAKMP/Oakley Toolkit	ANY	SW	ISAKMP	KIT	3DES
FRANCE	ActivCard	ActivCard X9.9 Token	PC	HW	COMMS	TOKEN	DES
FRANCE	Atlantis	CSA / X.25	X.25	SW/HW	COMMS	BOX	PROP
FRANCE	Bull Worldwide Information Systems Inc.	CP8 Log	WK	SW/HW	DISK	PGM	
FRANCE	Bull Worldwide Information Systems Inc.	OpenMaster	WIN/NT	SW	COMMS	PGM	DES
FRANCE	Bull Worldwide Information Systems Inc.	SecurWare VPN	ETHERNET	SW/HW	VPN	BOX	DES
FRANCE	CCETT	??					
FRANCE	CSEE - Division Communication et Informatique	??					
FRANCE	Dassault Automatismes et Telecommunications	??					
FRANCE	Digital Equipment Corp. (DEC). Pans Research Lab	RSA chip		HW		CHIP	RSA
FRANCE	Herve Schauer Consultants	HSC-GK (Gate Keeper)	UNIX				DES
FRANCE	Hewlett Packard France	Cryptographic Security Module for the HP9000	HP/UX	HW	GENERAL	SMART CARD	DES
FRANCE	LAAS	RSA implementations					RSA
FRANCE	Philips Communication Systems	P83C852 Smart Card Crypto Controller	TTL	HW	GENERAL	CHIP	RSA
FRANCE	Rast Electronics	Crypt It					
FRANCE	SAGEM	??					
GERMANY	Andreas Kupries	TCL Binary Large Objects eXtension(Tcl-BlobX) v1.2	TCL 7.5	SW	GENERAL	KIT	DES
GERMANY	Andreas Muller Software	??					
GERMANY	Baller & Huwig	Louis Cypher LC-1	telephone	HW	VOICE	BOX	RSA
GERMANY	BioData GmbH	Babylon Meta ISDN	RJ-45	HW	COMMS	BOX	3DES
GERMANY	BioData GmbH	Babylon Meta Serial	RJ-45	HW	COMMS	BOX	3DES
GERMANY	BioData GmbH	Babylon Standard	ISDN	HW	COMMS	BOX	3DES
GERMANY	BioData GmbH	BIGFire+	ETHERNET	HW	COMMS	BOX	3DES
GERMANY	BROKAT Infosystems AG	X*PRESSO Security Package 3.0	JAVA	SW	SSL	KIT	IDEA
GERMANY	CCI (Competence Center Informatik GmbH)	??					
GERMANY	CE Infosys GmbH	CD-Crypt	WIN32	SW	CD-ROM	PGM	3DES
GERMANY	CE Infosys GmbH	CryptCard	PC	HW	GENERAL	PCMCIA	DES
GERMANY	CE Infosys GmbH	DataCrypt	WIN32	SW/HW	FILE		3DES
GERMANY	CE Infosys GmbH	Elkey	PC	HW	DISK	BOX	DES
GERMANY	CE Infosys GmbH	Fastcrypt	PCI	HW	GENERAL	BOARD	DES
GERMANY	CE Infosys GmbH	IP-Crypt	WIN32	SW/HW	COMMS	PGM	3DES
GERMANY	CE Infosys GmbH	IPC-Box	UNIX	HW	COMMS	BOX	3DES
GERMANY	CE Infosys GmbH	PCI-Crypt	WIN32	HW	GENERAL	CHIP	3DES
GERMANY	CE Infosys GmbH	RSA Smart Card	PCMCIA	HW	COMMS	SMART CARD	3DES
GERMANY	CE Infosys GmbH	RSA-Crypt	WIN32	SW/HW	FILE	PGM	3DES
GERMANY	CE Infosys GmbH	Simo PCI/AT	WIN32	HW	GENERAL	BOARD	3DES
GERMANY	CE Infosys GmbH	SuperCrypt	TTL	HW	GENERAL	CHIP	DES
GERMANY	Cedric Reinartz	ASPiCryp		SW	FILE	PGM	BLOWFISH
GERMANY	Cellcon	Script	WIN	SW	DISK		DES
GERMANY	Christoph Martin	SSL-MZ telnet	UNIX	SW	TELNET	PGM	IDEA
GERMANY	CryptoSoft GmbH	Blowfish Development Kit	DOS	SW	GENERAL	KIT	BLOWFISH
GERMANY	CryptoSoft GmbH	DES3 Development Kit	DOS	SW	GENERAL	KIT	3DES
GERMANY	CryptoSoft GmbH	Enigma for Windows 98	WIN95	SW	FILE	PGM	DES
GERMANY	CryptoSoft GmbH	Enigma for Windows v 3.1	WIN	SW	FILE	PGM	DES
GERMANY	DataSafe	ENCRYPT-IT v3.06	PC	SW	FILE	PGM	DES
GERMANY	DataSafe	WINDEX! v2.01 for DOS	PC	SW	FILE	PGM	PROP
GERMANY	DataSafe	WINDEX! v2.01 for Windows	PC	SW	FILE	PGM	PROP
GERMANY	DemCom	Sieganos	WIN95	SW	FILE	PGM	PROP
GERMANY	DTM Data TeleMark GmbH	DICA 7800 ISDN Line Encryptor	ISDN	HW	COMMS	BOX	DES
GERMANY	EZI GmbH	H-Crypt		SW			FEAL
GERMANY	FAST ComTec GmbH	MACS 1000	PC	SW/HW	COMMS	PGM	DES
GERMANY	GAO	??					
GERMANY	Glas & Herweg	GH-DES		SW	FILE		DES
GERMANY	Glück & Kanja GmbH	CryptoEx Security Suite	WIN32	SW	EMAIL	PGM	IDEA
GERMANY	GMD	SecuDE PEM	UNIX	SW	EMAIL	PGM	DES
GERMANY	GMD	SECUDE-5.0	DOS	SW	GENERAL	KIT	
GERMANY	Interconnect	Babylon		HW	COMMS		DES
GERMANY	Interconnect	BIGfire	telephone	HW			DES
GERMANY	Jurgen Meyer, Frank Gadegast	SECMPEG		SW	VIDEO		DES
GERMANY	Karl Huwig	LC-1 Fax/Data Encryption Unit		HW	FAX	BOX	RSA
GERMANY	Karl Huwig	LC-1 Voice Encryption Unit	telephone	HW	VOICE	BOX	RSA
GERMANY	KryptoKom	KryptoGuard Modem	PC	HW	COMMS	BOX	DES
GERMANY	KryptoKom	KryptoGuard X.25	X.25	HW	GENERAL	BOX	DES
GERMANY	KryptoKom	KryptoServer	V.24	HW	GENERAL	BOARD	DES
GERMANY	KryptoKom	SmartGuard S	DOS	SW/HW	GENERAL	PGM	DES
GERMANY	Mathias Kretschmer	ProCrypt	AMIGA	SW	FILE	PGM	DES
GERMANY	Roland Mundloch	Azcrypt	WIN95	SW	FILE	PGM	PROP
GERMANY	Siemens Vertrauliche Kommunikation	ISDN - Channel			FILE VOICE		
GERMANY	Siemens-Nixdorf	??					DES
GERMANY	Siemens-Nixdorf	SESAME	UNIX	SW	COMMS	PGM	
GERMANY	Siemens-Nixdorf	SICURE		HW		CHIP	DES

GERMANY	Siemens-Nixdorf	Trusted Web		SW/HW	COMMS	PGM	
GERMANY	SIT	ComSave SIC 410	V.24	HW	COMMS	BOARD	PROP(FEAL 16X)
GERMANY	T. Billenstein	tbCrypt	DOS	SW	FILE	PGM	DES
GERMANY	Tela Versicherung	??					
GERMANY	Tele Security Timmann GmbH & Co.	TST 3010 High Performance Mil-Spec Cipher Terminal	RADIO	HW	COMMS	BOX	PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 3550 Handy Crypt	PRINTER	HW	COMMS	BOX	PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 3570 Pocketcrypt	telephone	HW	COMMS	BOX	PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 3677 VDU/Screen-Oriented Headquarter Cipher		HW	COMMS	BOX	PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 4043 HF Slow Speed Modem with encryption	PC	HW	COMMS	BOX	PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 4045 HF Modem 2.4Kbps with encryption	PC	HW	COMMS	BOX	PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 5500 Crypto Modem	PC	SW/HW	COMMS	BOX	PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 5560 DataCipher Set	RS232	HW	COMMS	BOX	PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 5573 C Data Encryptor	PC	HW	COMMS	BOX	PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 5573 F/C		HW	FAX		PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 5573 H/C		HW	COMMS	BOX	PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 5573 P/C		HW	COMMS	BOX	PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 5573 X/C		HW	COMMS	BOX	PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 7595 HF voice encryption	telephone	HW	VOICE	BOX	PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 7610 Secure Office Telephone	telephone	HW	VOICE	BOX	PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 7698 Miniature Military Voice Cocer	telephone	HW	VOICE	BOX	PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 7720 Telephone Vocoder and Modem	telephone	HW	VOICE	BOX	PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 8010 Spreadspectrum Radio	RS232	HW	COMMS	BOARD	PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 9659 Telex Cipher Module	TELEX	HW	COMMS	BOARD	PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 9700 INMARSAT "C" encryptor	PC	SW/HW	COMMS	BOX	PROP
GERMANY	Telenet Kommunikation Systeme	File Transfer	IBM/MVS	SW	FILE	KIT	DES
GERMANY	Toshiba Europe GmbH	CryptCard	PC	HW	DISK	PCMCIA	DES
GERMANY	Ulmaco Safeware AG	BACK-Guard	PC	SW	DISK	PGM	DES
GERMANY	Ulmaco Safeware AG	C:Crypt	PC	SW	FILE	PGM	PROP
GERMANY	Ulmaco Safeware AG	Cryptware Board 1.3		HW	EMAIL	BOARD	DES
GERMANY	Ulmaco Safeware AG	Cryptware Server 3.0		HW	COMMS	BOX	DES
GERMANY	Ulmaco Safeware AG	Cryptware Toolkit	ANY	SW	GENERAL	KIT	3DES
GERMANY	Ulmaco Safeware AG	PC/DACS for DOS + Windows	DOS	SW	FILE	PGM	
GERMANY	Ulmaco Safeware AG	SAFE-Board I	PC	HW	DISK	BOARD	XOR
GERMANY	Ulmaco Safeware AG	SAFE-Board II	PC	HW	DISK	BOARD	DES
GERMANY	Ulmaco Safeware AG	SAFE-Board III	PC	HW	DISK	BOARD	DES
GERMANY	Ulmaco Safeware AG	SAFE-Guard OS/2 3.0	PC	SW	DISK	PGM	DES
GERMANY	Ulmaco Safeware AG	SAFE-Guard Professional 3.2C	PC	SW	DISK	PGM	DES
GERMANY	Ulmaco Safeware AG	SafeGuard DACS for Windows 95	WIN95	SW	GENERAL	PGM	
GERMANY	Ulmaco Safeware AG	SafeGuard Desktop 2.10	OS2	SW	DISK	PGM	DES
GERMANY	Ulmaco Safeware AG	SafeGuard Easy 1.01	WIN/NT	SW	DISK	PGM	DES
GERMANY	Ulmaco Safeware AG	Safeguard Easy 1.13	WIN95	SW	DISK	PGM	DES
GERMANY	Ulmaco Safeware AG	SafeGuard Easy 2.18	OS2	SW	DISK	PGM	DES
GERMANY	Ulmaco Safeware AG	SafeGuard Easy 2.24	DOS	SW	DISK	PGM	DES
GERMANY	Ulmaco Safeware AG	SafeGuard LAN Crypt 1.0	WIN/NT	HW	COMMS	PGM	DES
GERMANY	Ulmaco Safeware AG	SafeGuard Professional 2.10	OS2	SW	DISK	PGM	DES
GERMANY	Ulmaco Safeware AG	SafeGuard Sign&Crypt	WIN32	SW	FILE	PGM	IDEA
GERMANY	Ulmaco Safeware AG	SafeGuard VPN	UNIX	SW	VPN	PGM	3DES
GERMANY	Ulmaco Safeware AG	SIGN-Guard	PC	SW	EMAIL VOICE	PGM	DES
GERMANY	Wilhelm Heibl Werke	??					
GREECE	John Ioannidis	JI's IPsec	BSD	SW	IPSEC	PGM	DES
HONG KONG	ROCTEC Enterprises, Ltd	??					
HONG KONG	Techtrend Engineering, Ltd. (TEL)	??					
HONG KONG	Triple D Ltd	P-8 Security Master Card	PC	SW/HW	GENERAL	PGM	DES
ICELAND	Logi Ragnarsson	Cryptonite Java Package	JAVA	SW	FILE	KIT	
ICELAND	Softis hf	LOUIS Security Package	JAVA	SW	COMMS	PGM	3DES
INDIA	Bharat Electronics Ltd	Analogue Code Encryption Unit	RADIO	HW	PW	BOX	
INDIA	Bharat Electronics Ltd	AZ7308 E Speech Encryption Unit	RADIO	HW	VOICE	BOX	
INDIA	Chenab Info Technology	Cryptic	PC	SW	FILE	PGM	PROP
IRAN	Communications Industries Group	AEU-212 Encryption Unit	RADIO	HW	VOICE	BOX	
IRAN	Communications Industries Group	AEU-313/A Encryption System	RADIO	HW	VOICE	BOX	
IRAN	Communications Industries Group	DEU-104 Digital Voice Encryption Unit	RADIO	HW	VOICE	BOX	
IRAN	Communications Industries Group	FEU-4110 Facsimile Encryption Unit	telephone	HW	FAX	BOX	
IRAN	Communications Industries Group	LEU-313 Telephone Encryption Unit	telephone	HW	VOICE	BOX	
IRAN	Communications Industries Group	TEU-520 Telex Encryption Unit	TELEX	HW	COMMS	BOX	
IRELAND	AT&T Network Systems Ireland	AT&T StrarLAN 10		SW			
IRELAND	Eurologic Systems, Ltd	Datacrypt	SCSI	HW	TAPE	BOX	PROP(BSA
IRELAND	Eurologic Systems, Ltd	DC-200	wk	HW	DISK	BOX	BSA
IRELAND	Key Exchange Ireland Ltd	??	PC				
IRELAND	Priority Data Systems Ltd	??					
IRELAND	Shamus Software Ltd.	??					
IRELAND	Silicon Software Systems Ltd.	??					
IRELAND	Software and Systems Engineering Ltd.	TrustedMIME	WIN95	SW	S/MIME	PGM	3DES
IRELAND	Software and Systems Engineering Ltd.	TrustedWeb Express	WIN95	SW	COMMS	PGM	
IRELAND	Software and Systems Engineering Ltd.	TrustedWeb v. 2.0	WIN95	SW	COMMS	PGM	3DES
IRELAND	Software Systems Engineering Ltd.	??					
IRELAND	Systemics Ltd.	Cryptix Cryptographic Library for Java 3.03	JAVA	SW	GENERAL	KIT	DES
IRELAND	Systemics Ltd.	Cryptix Java Cryptographic Extensions	JAVA	SW	GENERAL	KIT	DES
IRELAND	Systemics Ltd.	Elliptix	JAVA	SW	GENERAL	KIT	ECC
IRELAND	Systemics Ltd	PGP Library for Perl	PERL	SW	GENERAL	KIT	PGP
ISLE OF MAN	Invisimail International Ltd.	Invisimail V3.1	WIN	SW	EMAIL	PGM	RPK

ISRAEL	Aladdin Knowledge Systems, Ltd.	ASECrypto	WIN95	SW	FILE	KIT	DES
ISRAEL	Aladdin Knowledge Systems, Ltd.	HASP	DOS	HW			
ISRAEL	Algorithmic Research Ltd.	CryptoKit	DOS	SW	GENERAL	KIT	DES
ISRAEL	Algorithmic Research Ltd.	CryptoSafe		HW	KEYS		DES
ISRAEL	Algorithmic Research Ltd.	CryptoServer	ETHERNET	SW		SMART CARD	
ISRAEL	Algorithmic Research Ltd.	CryptoServer	ETHERNET	HW	GENERAL	BOX	DES
ISRAEL	Algorithmic Research Ltd.	PrivateWire	ETHERNET	SW/HW	COMMS	PGM	DES
ISRAEL	Alroo Ltd.	PrivaFile	WIN	SW	FILE	PGM	PROP
ISRAEL	Alroo Ltd.	PrivaMail	WIN	SW	EMAIL	PGM	PROP
ISRAEL	Alroo Ltd.	PrivaSoft	DOS	SW	FAX	PGM	PROP
ISRAEL	Carmel Software Engineering Ltd.	INFOLOCK	PC	SW	FILE	PGM	PROP
ISRAEL	CheckPoint Software Technologies Ltd	FireWall -1 4.0	UNIX	SW/HW	VPN	KIT	3DES
ISRAEL	CheckPoint Software Technologies Ltd	VPN-1 Accelerator Card	PCI BUS	HW	VPN	BOARD	DES
ISRAEL	CheckPoint Software Technologies Ltd	VPN-1 Appliance	V.35	HW	VPN	BOX	DES
ISRAEL	CheckPoint Software Technologies Ltd	VPN-1 SecuRemote	WIN95	SW	VPN	PGM	DES
ISRAEL	Elementrix Technologies Ltd.	POTP Secure FTP	WIN	SW		PGM	POTP
ISRAEL	Elementrix Technologies Ltd.	POTP Secure Mail	WIN	SW	EMAIL	PGM	POTP
ISRAEL	Ins Software	Comlock	UNIX				
ISRAEL	Ins Software	Imlock	UNIX				
ISRAEL	RADGUARD, Ltd	clPro-client	WIN32	SW	IPSEC	PGM	
ISRAEL	RADGUARD, Ltd	clPro-DMZ	ETHERNET	HW	IPSEC	BOX	DES
ISRAEL	RADGUARD, Ltd	clPro-HQ	ETHERNET	HW	IPSEC	BOX	3DES
ISRAEL	RADGUARD, Ltd	clPro-VPN	ETHERNET	HW	IPSEC	BOX	
ISRAEL	RADGUARD, Ltd	CryptoWall	ETHERNET	HW	COMMS	BOX	DES
ISRAEL	RADGUARD, Ltd	NetCryptor	X.25	HW	VPN	BOX	DES
ISRAEL	Secure Network Systems, Ltd.	Only You	DCS	HW	DISK	PCMCIA	
ISRAEL	Secure Network Systems, Ltd.	You & Me	DCS	HW	COMMS	PCMCIA	
ISRAEL	Tadiran	SEC-13					
ISRAEL	Tadiran	SEC-15					
ISRAEL	Tadiran	SEC-22					
ISRAEL	Vanguard Security Technologies Ltd	MailGuardian	WIN/NT	SW	EMAIL	PGM	DES
ITALY	AMTEC SPA	AMTEC SPA Cryptocard	PCMCIA	HW	COMMS	SMART CARD	RSA
ITALY	AMTEC SPA	Crypto Device	PC	HW	COMMS	BOARD	RSA
ITALY	AMTEC SPA	CryptoBox	X.25	HW	COMMS	BOX	RSA
ITALY	AMTEC SPA	CryptoFile	WIN95	SW/HW	FILE	PGM	RSA
ITALY	AMTEC SPA	CS-860	X.25	HW	IPSEC	BOARD	3DES
ITALY	AMTEC SPA	RSA 512		HW	COMMS	CHIP	RSA
ITALY	CERT-IT	STEL	SUNOS	SW	COMMS	PGM	DES
ITALY	Eutron Spa	SmartKey plus / GSS	DOS	SW/HW		KIT	PROP
ITALY	Eutron Spa	SmartKey plus Buss /GSS	DOS	SW/HW	FILE	KIT	PROP
ITALY	Eutron Spa	SmartLock BASE	LAN	SW	DISK	PGM	PROP
ITALY	Eutron Spa	SmartLock DEFence	DOS	SW	DISK	PGM	PROP
ITALY	Eutron Spa	SmartLock DEScryption	DOS	SW	DISK	PGM	DES
ITALY	Eutron Spa	SmartLock PROfessional	DOS	SW	DISK	PGM	PROP
ITALY	Systems Communicazioni srl	Secure Desk-Top	WIN	SW	FILE	PGM	DES
ITALY	Systems Communicazioni srl	Secure Plug-in for Eudora	WIN	SW	EMAIL	PGM	DES
ITALY	TELSY Elettronica e Telecomunicazioni S.p.A.	ALLFAX 1000		HW	FAX	BOX	PROP
ITALY	TELSY Elettronica e Telecomunicazioni S.p.A.	Cryptophone 7000	TELEPHONE	HW	COMMS		PROP
ITALY	TELSY Elettronica e Telecomunicazioni S.p.A	Cryptophone 7000 plus	TELEPHONE	HW	COMMS		PROP
ITALY	TELSY Elettronica e Telecomunicazioni S.p.A.	Cryptophone 7900		HW	COMMS	BOX	PROP
ITALY	TELSY Elettronica e Telecomunicazioni S.p.A.	KD111 C		HW	COMMS	BOX	PROP
ITALY	TELSY Elettronica e Telecomunicazioni S.p.A	KV3000		HW	COMMS	BOX	PROP
ITALY	TELSY Elettronica e Telecomunicazioni S.p.A.	TX1020 C Mk III		HW	COMMS	BOX	PROP
ITALY	TELSY Elettronica e Telecomunicazioni S.p.A.	TX2020 C		HW	COMMS	BOX	PROP
JAPAN	ADVANCE Co., Ltd	KPS Cipher Card		HW			
JAPAN	Compal Inc.	Pandora		HW	GENERAL	CHIP	DES
JAPAN	Fujitsu Labs Ltd.	FJPEM v1.0	MANY	SW	EMAIL	PGM	DES
JAPAN	Mitsubishi Electric Corporation	CERTMANAGER v.B00	WIN32	SW	S/MIME	PGM	MISTY1
JAPAN	Mitsubishi Electric Corporation	CertMISTY V.B00	WIN32	SW	GENERAL	PGM	MISTY1
JAPAN	Mitsubishi Electric Corporation	Cryptofile vB00	WIN32	SW	DISK	PGM	MISTY1
JAPAN	Mitsubishi Electric Corporation	CryptoSign v.B00	WIN32	SW	EMAIL	PGM	MISTY1
JAPAN	Mitsubishi Electric Corporation	MELWALL A3000-1	ETHERNET	HW	COMMS	BOX	MISTY1
JAPAN	Mitsubishi Electric Corporation	MELWALL H3000-1	ETHERNET	HW	COMMS	BOX	MISTY1
JAPAN	Mitsubishi Electric Corporation	MELWALL P3000 v.E00	WIN32	SW	COMMS	PGM	MISTY1
JAPAN	Mitsubishi Electric Corporation	MELWALL P3000CL	WIN95	SW	COMMS	PGM	MISTY1
JAPAN	Mitsubishi Electric Corporation	PowerMisty v.B00	WIN/NT	SW	GENERAL	KIT	MISTY1
JAPAN	Mitsubishi Electric Corporation	TrustWeb v.B00	WIN32	SW	COMMS	PGM	MISTY1
JAPAN	Mitsubishi Electric Engineering Company Ltd	MISTYKEYPER v.B00	WIN/NT	SW/HW	KEYS	BOARD	MISTY1
JAPAN	Nihon RSA	RSA Chip		HW	GENERAL	CHIP	RSA
JAPAN	Nihon Telephone & Telegraph	Encryption Chip	ANY	HW	GENERAL	CHIP	3DES
JAPAN	Toshiba Information Systems (Japan)	Cypher Mail	WIN95	SW	EMAIL	PGM	
JAPAN	Yokohama National University	KPS L1CARD					
KOREA	Future Systems, Inc.	Future/TCP v4.0	DOS	SW	COMMS	PGM	DES
KOREA	JiranSoft	FileSafe v1.0	PC	SW	FILE	PGM	BLOWFISH
KOREA	Penta Security Systems Inc.	ISSAC v. 1.0	ANY	SW	GENERAL	KIT	PROP
KOREA	Senex Technologies Inc. Ltd	Assure Web CA	WIN/NT	SW		PGM	RSA
KOREA	Senex Technologies Inc. Ltd	Assure X-filer for WorkGroup v3.0	WIN	SW	FILE	PGM	BLOWFISH
KOREA	Senex Technologies Inc. Ltd	Assure X-Mailer	WIN	SW	FILE	PGM	BLOWFISH

KOREA	SoftForum	XecureDoc 1.0	WIN32	SW	FILE	PGM	RC4
KOREA	SoftForum	XecureMail 2.0	WIN32	SW	EMAIL	PGM	RC4
KOREA	SoftForum	XecureWeb 3.0	WIN	SW	COMMS	PGM	RC4
MEXICO	Seguridata Privada S.A. de C.V.	SegurDOC	WIN	SW	FILE	PGM	3DES
MEXICO	Seguridata Privada S.A. de C.V.	SegurEDIFACT	JAVA	SW	EDI	PGM	3DES
MEXICO	Seguridata Privada S.A. de C.V.	SegurLIB	C CODE	SW	GENERAL	KIT	3DES
MEXICO	Seguridata Privada S.A. de C.V.	SegurPROXY	WIN32	SW	COMMS	PGM	RC4
MEXICO	Seguridata Privada S.A. de C.V.	SegurTELNET	WIN32	SW	COMMS	PGM	RC4
MEXICO	The King of Hearts	Potassium Hydroxide (KOH)	DOS	SW	DISK		IDEA
NETHERLANDS	Ad Infinitum Programs (AIP-NL)	UltraCompressor II	PC	SW	FILE	PGM	DES
NETHERLANDS	Alloo Blom Software	Web Confidential	MAC	SW	PW	PGM	BLOWFISH
NETHERLANDS	Ascii B.V.	ThunderCrypt	WIN/NT	SW	FILE	PGM	BLOWFISH
NETHERLANDS	Ascii B.V.	ThunderSafe	WIN/NT	SW	FILE	PGM	BLOWFISH
NETHERLANDS	Concord Eracom Nederland BV	DEA Crypto Toolkit	PC	SW	GENERAL	KIT	DES
NETHERLANDS	Concord Eracom Nederland BV	Multi-Functional PC Security (MFPS) Card	PC	HW	GENERAL	BOARD	DES
NETHERLANDS	Concord Eracom Nederland BV	SCORE	PC	SW	GENERAL	KIT	DES
NETHERLANDS	Concord Eracom Nederland BV	SECNET (FCM)	PC	SW/HW	DISK		DES
NETHERLANDS	Concord Eracom Nederland BV	SECNET (HCM)	PC	HW	DISK	BOARD	DES
NETHERLANDS	Concord Eracom Nederland BV	SECNET (SCM)	PC	SW	DISK	PGM	DES
NETHERLANDS	Concord Eracom Nederland BV	SECNET FBI-Encryptor	PC	HW	GENERAL	BOARD	DES
NETHERLANDS	Concord Eracom Nederland BV	SECNET MFPS	PC	SW/HW	COMMS	PGM	DES
NETHERLANDS	Concord Eracom Nederland BV	SECNET PC SoftLock 4.5	PC	SW	DISK	PGM	
NETHERLANDS	DigiCash	Electronic cash systems					
NETHERLANDS	DigiCash	Electronic toll payment systems					
NETHERLANDS	DigiCash	Infor Guard i-1200 (The Krypter)	DOS	SW/HW	GENERAL	PGM	DES
NETHERLANDS	Inaaa Datacom BV	AUTHORIZER	RS232	HW	COMMS	BOX	PROP
NETHERLANDS	Philips Crypto B.V.	PFDX 2035 Fax Encryptor	FAX	HW	COMMS	SMART CARD	PROP(high end)
NETHERLANDS	Philips Crypto B.V.	PNVX 2116 Crypto Switch	FBX	HW	COMMS	BOX	
NETHERLANDS	Philips Crypto B.V.	PNVX 2118 Secure Telephone	RS232	HW	COMMS	SMART CARD	PROP(high end)
NETHERLANDS	Philips Crypto B.V.	PPSX 2061 Data Encryptor	X.25	HW	COMMS	BOX	DES
NETHERLANDS	Philips Crypto B.V.	Vkaart	WIN/NT	SW/HW	FILE	PCMCIA	
NETHERLANDS	Pijnenburg	PCC100 Bulk Data Encryptor Chip	TTL	HW	GENERAL	CHIP	DES
NETHERLANDS	Pijnenburg	PCC100 High Speed DES Chip	TTL	HW	GENERAL	CHIP	DES
NETHERLANDS	Pijnenburg	PCC101	ANY	HW	GENERAL	CHIP	DES
NETHERLANDS	Pijnenburg	PCC200 RSA Chip	TTL	HW	GENERAL	CHIP	RSA
NETHERLANDS	Pijnenburg	PCC201	ANY	HW	GENERAL	CHIP	DES
NETHERLANDS	Tulip Computers BV	Disk Encryption Unit					
NETHERLANDS	Verspeck & Soeters b.v.	SecurIO	ANY	HW	COMMS	BOARD	DES
NETHERLANDS	Verspeck & Soeters B.V.	SecurIO I	ANY	HW	COMMS	BOX	DES
NETHERLANDS	Verspeck & Soeters B.V.	SecurIO II	ANY	HW	COMMS	BOX	
NETHERLANDS	Verspeck & Soeters B.V.	SecurIO III	ANY	HW	COMMS	BOX	DES
NEW ZEALAND	CES Communications Ltd.	Elite2000 XL	TTL	HW	FAX		PROP
NEW ZEALAND	CES Communications Ltd.	Elite2000 XT	TTL	HW	VOICE	PHONE	PROP
NEW ZEALAND	CES Communications Ltd.	Fax Guardian	TTL	HW	FAX		PROP
NEW ZEALAND	CES Communications Ltd.	Phone Guardian	TTL	HW	VOICE		PROP
NEW ZEALAND	John Gilmore	Free SWAN 1.00	LINUX	SW	COMMS	PGM	3DES
NEW ZEALAND	LUC Encryption Technology, Ltd. (LUCENT)	LCF Library	ANY	SW	GENERAL	KIT	LUC
NEW ZEALAND	LUC Encryption Technology, Ltd. (LUCENT)	slir	PC	SW	FILE	PGM	LUC
NEW ZEALAND	Peter Gutmann	Cryptlib		SW	GENERAL	KIT	<SEE NOTES>
NEW ZEALAND	Peter Gutmann	HPACK Archiver 0.79	PC	SW	FILE	PGM	MDC
NEW ZEALAND	Peter Gutmann	Secure File System (SFS) 1.1	PC	SW	DISK	PGM	MDC
NEW ZEALAND	RPK New Zealand	Invismail Professional	WIN95	SW	EMAIL	PGM	RPK
NEW ZEALAND	RPK New Zealand	RPK File 1.01	WIN	SW	FILE	PGM	RPK
NEW ZEALAND	RPK New Zealand	RPK Public Key Cryptosystem	UNIX	SW	GENERAL	KIT	RPK
NEW ZEALAND	RPK New Zealand	TRPKC	WIN	SW	GENERAL	KIT	RPK
NEW ZEALAND	RPK New Zealand Ltd	RPK Encryptonite Software Toolkit V3.1	C++ CODE	SW	GENERAL	KIT	RPK
NEW ZEALAND	RPK New Zealand Ltd	RPK SecureMedia V1.0	WIN/NT	SW	MEDIA	PGM	RPK
NORWAY	Aftadn Software	??					
NORWAY	Columbi Micro a.s	??					
NORWAY	Ericsson Semafor	??					
NORWAY	InfoMedica AS	??					
NORWAY	Informasjonskontroll A/S	??					
NORWAY	Informatikk A/S	??					
NORWAY	Kirkedam Elektronikk EDB	??					
NORWAY	Ness A.S.	??					
NORWAY	Scand PC Sys/Sectra	??					
NORWAY	Siemens Nixdorf Informationssystemer A/S	??					
NORWAY	Sterling Software Scandinavia A/S	??					
NORWAY	Telepartner as	??					
NORWAY	Vectech A.S.	??					
POLAND	Enigma Information Security Systems	PEM - HEART	PC	SW	EMAIL	PGM	DES
ROMANIA	Interscope s.r.l.	Interscope Blackbox	WIN/NT	SW	FILE	PGM	DES
RUSSIA	Ancort	Ancrypt		HW	GENERAL	BOX	PROP
RUSSIA	Ancort	Cryptocenter Version 1.5	PC	SW	FILE	PGM	PROP
RUSSIA	Ancort	CryptoGrapher	WIN/CE	SW	GENERAL	PGM	PROP
RUSSIA	Ancort	Cyberdog	WIN95	SW	FILE	PGM	PROP
RUSSIA	Ancort	File Cipher	WIN95	SW	FILE	PGM	PROP
RUSSIA	Askri	Cryptos	PC	SW	FILE	PGM	DES
RUSSIA	Elas Ltd	Excellence for DOS	PC	SW	FILE	PGM	GOST
RUSSIA	INFORM - RTG	Absolute Cryptographer	ANY	SW	GENERAL	PGM	PROP
RUSSIA	LAN Crypto	CRYPTOBANK (NOTARY & VESTA utilites)	UNIX	SW	DISK	KIT	DES
RUSSIA	LAN Crypto	DIANA	WK	SW	LAN	KIT	
RUSSIA	LAN Crypto	Orus	DOS	SW	FILE	KIT	DES

RUSSIA	LAN Crypto	Sphinx	PC	SW	DISK	PGM	
RUSSIA	LAN Crypto	VESTA	UNIX	SW	DISK	KIT	DES
RUSSIA	RESCrypto	??		HW		BOARD	GOST
RUSSIA	ScanTech	Krypton		SW	FILE	PGM	DES
RUSSIA	TELECRYPT, Ltd.	TELECRYPT	PC	SW	VPN	PGM	DES
SOUTH AFRICA	Citadel Data Security	Citadel Firewall	UNIX	SW			
SOUTH AFRICA	Computer Security Associates	??					
SOUTH AFRICA	Denel Informatics	IWATCH	PC	SW	COMMS	PGM	DES
SOUTH AFRICA	EFT	??		HW		BOARD	DES
SOUTH AFRICA	Intelligent	??		HW	COMMS	BOX	
SOUTH AFRICA	Nanoteq	??					
SOUTH AFRICA	Net One	??					
SOUTH AFRICA	NetSec	Application Gateway	PC	SW	COMMS	PGM	DES
SOUTH AFRICA	NetSec	NetSec Manager		SW		PGM	DES
SOUTH AFRICA	NetSec	Secure Router		SW	COMMS	KIT	DES
SOUTH AFRICA	Sentera	N3000M		HW			
SOUTH AFRICA	Siemens Ltd. So. Africa -Pretoria	??					
SOUTH AFRICA	Spescom	??					
SOUTH AFRICA	Thawte Consulting	Thawte Personal Certificate	MANY	SW	S/MIME		IDEA
SOUTH AFRICA	Thawte Consulting	Thawte SSL Server Certificate	MANY	SW	S/MIME		DES
SPAIN	SECARTYS	??					
SWEDEN	Ardy Elektronics	SLD/OUS-200	RS232	HW	COMMS	BOX	PROP(ARDY)
SWEDEN	Ardy Elektronics	SLF 2000	telephone	HW	FAX		PROP(ARDY)
SWEDEN	Ardy Elektronics	SLP 2000	telephone	HW	VOICE		PROP(ARDY)
SWEDEN	AU-System Communication AB	Avi - Boks	PC	SW/HW	COMMS	PGM	DES
SWEDEN	AV System Infocard	??	PC	SW/HW	DISK	KIT	RSA
SWEDEN	Business Security AB	Securefile	PCMCIA	HW	FILE	SMART CARD	PROP(SBLH-E)
SWEDEN	Business Security AB	SecuriCrypto G.703/704		HW	COMMS	BOX	PROP
SWEDEN	Business Security AB	SecuriCrypto V.24 S	V.24	HW	COMMS	BOX	PROP(STREAM)
SWEDEN	Business Security AB	SecuriCrypto V.24A (Asynchronous)	V.24	HW	COMMS	BOX	PROP(STREAM)
SWEDEN	Business Security AB	SecuriCrypto V.24S / V.24SR (Synchronous)	V.24	HW	COMMS	BOX	PROP(STREAM)
SWEDEN	Business Security AB	SecuriCrypto V.35 / V.35R	V.35	HW	COMMS	BOX	PROP
SWEDEN	Business Security AB	SecuriCrypto V.36	V.36	HW	COMMS	BOX	PROP(STREAM)
SWEDEN	Business Security AB	SecuriCrypto X.21, Datex	X.27	HW	COMMS	BOX	PROP(STREAM)
SWEDEN	Business Security AB	SecuriCrypto X.25	X.21bis	HW	COMMS	BOX	PROP(STREAM)
SWEDEN	Business Security AB	SecuriCrypto X.28	V.24	HW	COMMS	BOX	PROP
SWEDEN	Business Security AB	SecuriFax		HW	FAX	FAX	PROP(STREAM)
SWEDEN	Business Security AB	SecuriModem	V.34	HW	COMMS	MODEM	PROP(SBLH-E)
SWEDEN	Business Security AB	SecuriVideo	V.35	HW	VIDEO	BOX	PROP(SBLH-E)
SWEDEN	Business Security AB	SecuriVoice	telephone	HW	VOICE	SMART CARD	PROP(STREAM)
SWEDEN	COST Computer Security Technologies International	COST SCS	PC	SW/HW	GENERAL	TOKEN	DES
SWEDEN	COST Computer Security Technologies International	COST-EDI	PC	SW	COMMS		DES
SWEDEN	COST Computer Security Technologies International	COST-EKS	PC	SW	FILE		DES
SWEDEN	COST Computer Security Technologies International	COST-PEM	PC	SW	EMAIL	PGM	DES
SWEDEN	COST Computer Security Technologies International	Generalized Security Library (GSL)	PC	SW	GENERAL	PGM	DES
SWEDEN	DynaSoft	Avi-BoKs	PC	SW/HW	FILE	PGM	DES
SWEDEN	DynaSoft	BoKS 4.2	UNIX	SW/HW	COMMS	PGM	DES
SWEDEN	DynaSoft	Boks Connect	UNIX	SW	COMMS	PGM	RSA
SWEDEN	DynaSoft	Boks Desktop	WIN	SW	FILE	PGM	
SWEDEN	Henry Padilla	GHOST File Manager v. 3.0	WIN95	SW	FILE	PGM	DES
SWEDEN	SECTRA AB	FKK 930 - G.703/G.704/G.751		HW		BOX	KM3
SWEDEN	SECTRA AB	KK 621 - ISA		HW		BOARD	KM3
SWEDEN	SECTRA AB	KK 621 - PCCARD		HW		PCMCIA	DES
SWEDEN	SECTRA AB	KM3		HW		CHIP	KM3
SWEDEN	SECTRA AB	KryptoLan KLB 1002		HW		BOX	DES
SWEDEN	SECTRA AB	KryptoLan KLB 2020 - V. 35/ IP		HW		BOX	KM3
SWEDEN	SECTRA AB	KryptoLan KLS 1001		HW		BOX	DES
SWEDEN	SONNOR Crypto AB	HR&S	ANY	SW	COMMS	PGM	PROP(HR&S)
SWEDEN	SONNOR Crypto AB	PCrypt	ANY	SW	FILE	PGM	PROP(HR&S)
SWEDEN	Stig Ostholm	DES Implementation 2.2	ANY	SW	GENERAL	PGM	DES
SWITZERLAND	ASCOM Tech AG	IDEA Toolkit	ANY	SW	GENERAL	KIT	IDEA
SWITZERLAND	ASCOM Tech AG	VINCI	TTL	HW	GENERAL	CHIP	IDEA
SWITZERLAND	Brown-Boveri	??					
SWITZERLAND	Crypto AG	CRYPTOCOM HC-265	RADIO	HW	VOICE	BOX	
SWITZERLAND	Crypto AG	CRYPTOMATIC HC 5700 / 5750		SW/HW	COMMS	KIT	
SWITZERLAND	Crypto AG	CRYPTOVOX HC-3300	telephone	HW	VOICE	PHONE	
SWITZERLAND	Crypto AG	CSE-160 Secure Handheld Radio	RADIO	HW	VOICE	RADIO	
SWITZERLAND	Crypto AG	CSE-960 Secure Mobile Radio	RADIO	HW	VOICE	BOX	
SWITZERLAND	Crypto AG	HC-2203 PSTN Voice Encryption	TELEPHONE	HW	VOICE	BOX	
SWITZERLAND	Crypto AG	HC-2403 Secure GSM	CELL PHONE	HW	VOICE	PHONE	
SWITZERLAND	Crypto AG	HC-3460 Radio Voice Encryption	RADIO	HW	VOICE	BOARD	
SWITZERLAND	Crypto AG	HC-4220 Facsmile Encryption	FAX	HW	FAX	BOX	

SWITZERLAND	Crypto AG	HC-5250 Secure Hand-Held Terminal	PHONE	HW	COMMS	TERMINAL	
SWITZERLAND	Crypto AG	HC-5500 Secure Email		SW/HW	EMAIL		
SWITZERLAND	Crypto AG	HC-5700 Secure Emmission Protected Terminal	TELEPHONE	HW	COMMS	TERMINAL	
SWITZERLAND	Crypto AG	HC-6830 Secure Field Communication Terminal	PHONE	HW	COMMS	TERMINAL	
SWITZERLAND	Crypto AG	HC-6950 Secure Emmission Protected WorkStation	PC	HW	DISK	PC	
SWITZERLAND	Crypto AG	HC-6950 Secure WorkStation System	WIN	SW/HW	DISK	PC	
SWITZERLAND	Crypto AG	HC-7210/7220 Secure Modem		HW	COMMS	MODEM	
SWITZERLAND	Crypto AG	HC-7305/7310 ISDN Encryption		HW	COMMS	BOX	
SWITZERLAND	Crypto AG	HC-7500 Link Encryptor	V.24	HW	COMMS	BOX	
SWITZERLAND	Crypto AG	HC-7550 Multi-Link Bulk Encryptor	EUROCOM D/I	HW	COMMS	BOX	
SWITZERLAND	Crypto AG	HC-7820 VPN Encryption	ENET	HW	VPN	BOX	PROP
SWITZERLAND	Crypto AG	HC-7830 VPN Encryption	WINNT	HW	VPN	PCMCIA	PROP
SWITZERLAND	Crypto AG	HC-7910 ATM Encryption	ENET	HW	ATM	BOX	
SWITZERLAND	Crypto AG	KHC-1500 Key Handling Center	WIN	HW	DISK	PC	
SWITZERLAND	Crypto AG	SECOS 400/610 Secure VHF/UHF Frequency Hopping System	RADIO	HW	VOICE	BOX	
SWITZERLAND	Crypto AG	TFP-3400 Digital Telephony Gateway		HW	VOICE	BOX	
SWITZERLAND	ETH Zurich	ENskip	UNIX	SW	IPSEC	PGM	DES
SWITZERLAND	Gretacoder Data Systems AG	Gretacoder 522	RS232	HW	COMMS	BOX	DES
SWITZERLAND	Gretacoder Data Systems AG	Gretacoder 524	RS232	HW	COMMS	BOX	DES
SWITZERLAND	Gretacoder Data Systems AG	Gretacoder 526	X.21	HW	COMMS	BOX	DES
SWITZERLAND	Gretacoder Data Systems AG	Gretacoder 545	RS232	HW	COMMS	BOX	DES
SWITZERLAND	Gretacoder Data Systems AG	Gretacoder 549	X.25	SW/HW	COMMS	PGM	DES
SWITZERLAND	Gretacoder Data Systems AG	Gretacoder 605	V.35	HW	COMMS	BOX	DES
SWITZERLAND	Gretacoder Data Systems AG	Gretacoder 705 Authenticator	RS232	HW	GENERAL	BOX	RSA
SWITZERLAND	Gretacoder Data Systems AG	Gretacoder 710 Authenticator	X.25	HW	GENERAL	BOX	DES
SWITZERLAND	Lightning Instrumentation SA	Multicom Software Release 2.1		SW	COMMS	PGM	IDEA
SWITZERLAND	Omnisec AG	Omnicard	WIN95	SW/HW	FILE	PGM	
SWITZERLAND	Omnisec AG	Omnisec 212 - Secure Telephone for PSTN	TELEPHONE	HW	VOICE	PHONE	
SWITZERLAND	Omnisec AG	Omnisec 212 A2 - Secure Telephone for PSTN Server Version	TELEPHONE	HW	VOICE	PHONE	
SWITZERLAND	Omnisec AG	Omnisec 213 - Secure Telephone for ISDN	TELEPHONE	HW	VOICE	PHONE	
SWITZERLAND	Omnisec AG	Omnisec 510	PC	HW	COMMS	BOX	PROP
SWITZERLAND	Omnisec AG	Omnisec 520 - Facsmile Encryptor	FAX	HW	FAX	FAX	
SWITZERLAND	Omnisec AG	Omnisec 545 - X.25 Data Encryptor	V.24	HW	COMMS	BOX	PROP
SWITZERLAND	Omnisec AG	Omnisec 610	RS232	HW	COMMS	BOX	PROP
SWITZERLAND	Omnisec AG	Omnisec 620	RS232	HW	COMMS	BOX	PROP
SWITZERLAND	Omnisec AG	Omnisec 621 - Field Wire Encryptor	EUROCOM D/I	HW	COMMS	BOX	
SWITZERLAND	Omnisec AG	Omnisec 630	RS449	HW	COMMS	BOX	PROP
SWITZERLAND	Omnisec AG	Omnisec 640	V.10	HW	COMMS	BOX	PROP
SWITZERLAND	Omnisec AG	Omnisec 644 - Multi-Link Encryption System		HW	COMMS	BOX	
SWITZERLAND	Omnisec AG	Omnisec 650 - High-Speed Link Encryptor	ETHERNET	HW	COMMS	BOX	
SWITZERLAND	Omnisec AG	Omnisec 670 - Encrypting Modem	V.17	HW	COMMS	MODEM	
SWITZERLAND	Omnisec AG	Omnisec 910 - Secure Message Field Terminal	RADIO	HW	COMMS	TERMINAL	
SWITZERLAND	Organa	mProtect					
SWITZERLAND	Safeware AG	SAFE-BOARD	ISA	HW	COMMS	BOARD	DES
SWITZERLAND	Safeware AG	SAFE-DISK	DOS	SW/HW	DISK	PGM	DES
SWITZERLAND	Safeware AG	SAFE-FILE	DOS	SW/HW	FILE	PGM	DES
SWITZERLAND	Theissen Security Systems Ltd.	Thss-PC	OS2	SW	FILE	PGM	DES
TURKEY	ASELSAN Inc.	2010 Data Crypto Equipment	V.10	HW	COMMS	BOX	PROP
TURKEY	ASELSAN Inc.	2020 Packet Crypto Equipment	X.25	HW	COMMS	BOX	PROP
TURKEY	ASELSAN Inc.	2025 Network Management system	X.25	SW/HW	COMMS	PC	PROP
TURKEY	ASELSAN Inc.	2101 Integrated Voice and Data Encryptor	RJ-11	HW	COMMS	BOX	
UK	Adam Back	Export-a-Crypto-System sig	UNIX	SW	GENERAL	PGM	RSA
UK	Andrew Brown	Wincrdl	WIN	SW	GENERAL	PGM	DES
UK	Apricot Computers, Ltd.	APRICOT SECURITY SYSTEM, Release 5	PC	SW/HW	DISK	<See Notes>	
UK	Avant Guardian Ltd.	Proscriptor Security System	V.32	SW/HW	COMMS	BOX	Avant Guardian
UK	Baltimore Technologies plc.	C/SSL	SOLARIS	SW	SSL	KIT	DES
UK	Baltimore Technologies plc.	CG5000	ETHERNET	HW	COMMS	BOX	DES
UK	Baltimore Technologies plc.	Crypto Systems ToolKit v6.0	ANY	SW	COMMS	KIT	DES
UK	Baltimore Technologies plc.	ECS DeskTop	WINNT	SW	FILE	PGM	DES
UK	Baltimore Technologies plc.	ECS Server		SW		PGM	DES
UK	Baltimore Technologies plc.	ED2048R3 Rambutan	X.21	HW	COMMS	BOX	RAMBUTAN
UK	Baltimore Technologies plc.	ED8000RL	ETHERNET	HW	COMMS	BOX	RAMBUTAN
UK	Baltimore Technologies plc.	FileSecure 4.0		SW	FILE	PGM	DES
UK	Baltimore Technologies plc.	FormSecure 4.0		SW	COMMS	PGM	DES
UK	Baltimore Technologies plc.	HSP4000-Assure	WINNT	SW/HW	GENERAL	KIT	DES
UK	Baltimore Technologies plc.	J/Crypto 3.3	<SEE NOTES>	SW	GENERAL	KIT	DES
UK	Baltimore Technologies plc.	J/SSL	JAVA	SW	SSL	KIT	DES
UK	Baltimore Technologies plc.	MailSecure	<SEE NOTES>	SW	S/MIME	PGM	3DES
UK	Baltimore Technologies plc.	MailSecure Enterprise		SW	EMAIL	PGM	3DES
UK	Baltimore Technologies plc.	PKI-Plus SDK	ANY	SW	GENERAL	KIT	DES
UK	Baltimore Technologies plc.	WebSecure	<SEE NOTES>	SW	COMMS	PGM	
UK	Ben Laurie	Apache SSL		SW	COMMS	KIT	DES
UK	British Telecom	BT Lektor 3620 PC Secure v 3.02	PC	SW	FILE	PGM	PROP(B-CRYPT)
UK	British Telecom	BT Lektor 3620 PC Secure v1.1	PC	SW	FILE	PGM	RAMBUTAN
UK	British Telecom	RSA chip	TTL	HW	GENERAL	CHIP	RSA
UK	Business Simulations	Ultralock					

UK	Cambridge Electric Industries	??					
UK	Codepoint Systems Ltd.	??					
UK	Computer Security Ltd.	Safe Guard Systems					
UK	Data Innovation Ltd.	CS500	V.24	HW	COMMS	BOX	DES
UK	Data Innovation Ltd.	E32048	G703	HW	VOICE	BOX	DES
UK	Data Innovation Ltd.	ED500	V.24	HW	COMMS	BOX	DES
UK	Data Innovation Ltd.	ED600	V.24	HW	COMMS	BOX	PROP
UK	Data Innovation Ltd.	ED600R		HW	COMMS	BOX	RAMBUTAN
UK	Data Innovation Ltd.	Network Security Workstation (NSW)	PC	SW/HW	KEYS		DES
UK	Data Innovation Ltd.	PSP400	PC	HW	GENERAL	BOARD	DES
UK	DataSoft International Ltd.	DataCode		SW	GENERAL	KIT	BAZARIES
UK	DataSoft International Ltd.	DataTalk		SW	COMMS	PGM	BAZARIES
UK	Digital Crypto	Iris	DOS	SW	DISK	PGM	DES
UK	Digital Crypto	OS2-IRIS	OS2	SW	FILE	PGM	DES
UK	Digital Crypto	PC-IRIS V4.0 - 2	PC	SW	FILE	PGM	DES
UK	Digital Crypto	PC-MERLIN V2.0 - 1	PC	SW	FILE	PGM	DES
UK	Digital Crypto	VMS-IRIS	VMS	SW	FILE	PGM	DES
UK	Emergent Technologies, Ltd.	Eurokey Personal Edition	WIN/NT	SW	FILE	PGM	IDEA
UK	Emergent Technologies, Ltd.	Eurokey Professional Edition	WIN/NT	SW	FILE	PGM	IDEA
UK	Ewen Associates Limited	Cryptix Security Toolkit	ANY	SW	GENERAL	KIT	DES
UK	Ewen Associates Limited	SimpliCrypt for Windows	WIN/NT	SW	FILE	PGM	DES
UK	Fauzan Mirza	IDEA86	PC	SW	GENERAL	PGM	IDEA
UK	Finansa	Winmail		SW	EMAIL		LUCIFER
UK	Fulcrum Communications	??					
UK	GEC-Marconi Secure Systems	DATALOK H	ANY	HW	COMMS	BOX	PROP
UK	GEC-Marconi Secure Systems	DATALOK L	ANY	HW	COMMS	BOX	PROP
UK	GEC-Marconi Secure Systems	FAXLOK	ANY	HW	FAX	BOX	PROP
UK	GEC-Marconi Secure Systems	IC-H10SR	RADIO	HW	VOICE	BOX	PROP
UK	GEC-Marconi Secure Systems	IC-RP1510SR	RADIO	HW	VOICE	BOX	PROP
UK	GEC-Marconi Secure Systems	IC-V200SR	RADIO	HW	VOICE	BOX	PROP
UK	GEC-Marconi Secure Systems	Marcrypt		HW		CHIP	PROP(MARCRYPT)
UK	GEC-Marconi Secure Systems	MASC Crypto Management System	PC	SW/HW	COMMS	BOX	PROP
UK	GEC-Marconi Secure Systems	MASC Module	RADIO	HW	VOICE	ADAPTOR	PROP
UK	GEC-Marconi Secure Systems	SDT-100	telephone	HW	VOICE	BOX	PROP
UK	Gelosia	??					
UK	Global CIS Ltd.	Safeguard Security System	PC	SW	FILE	PGM	PROP
UK	Honeywell	??		SW			FEAL8
UK	ICL Secure Systems	TEAMcrypto					
UK	InfoShare	Omnidata	PC	SW	GENERAL	PGM	
UK	Instant Access	Digital Vault	MAC	SW	FILE	PGM	
UK	Interconnections	??					
UK	International Data Security, Ltd.	DataSave-ABA					
UK	International Data Security, Ltd.	Protec Net V4.1	DOS	SW	COMMS	PGM	
UK	International Data Security, Ltd.	Protec V4.1	DOS	SW	FILE	PGM	
UK	IQ International	Stealth		SW			PROP(HMX+)
UK	IT Security International	Secure LAN					
UK	ITV	??					
UK	J.R Ward Computers Ltd.	Code-II	PC	SW	FILE	PGM	PROP
UK	J.S.A. Kapp	RSAEURO 1.04 (Internet)	ANY	SW	GENERAL	KIT	DES
UK	J.S.A. Kapp	RSAEURO 1.10 (Commercial)	ANY	SW	GENERAL	KIT	DES
UK	Jaguar Communications Ltd.	ZCODA-A	RS232	HW	COMMS	BOX	PROP
UK	Jaguar Communications Ltd.	ZCODA-X	RS232	HW	COMMS	BOX	PROP
UK	Janus Sovereign	Padlock					
UK	JCP Computer Services	Crypto v2.0	JAVA	SW	GENERAL	KIT	DES
UK	JPY Associates Ltd	DataLock, Version 4.0	MF	SW	DISK	PGM	DES
UK	Loadplan	??					
UK	Logica	??					
UK	Microft Technology Ltd.	CLAM	PC	SW	FILE	PGM	PROP
UK	NEST Ltd.	CaGey Bee	WIN				
UK	Network Systems Corporation (UK)	Data Delivery/Management System					
UK	Novell, Ltd. (UK)	Trusted Netware 4		SW	COMMS	KIT	
UK	PC Security Ltd.	CP8-AuthentCC	PC	HW	FILE	SMART CARD	PROP
UK	PC Security Ltd.	LapGUARD	PC	SW	FILE	PGM	PROP
UK	PC Security Ltd.	Stoplock 95	WIN98	SW	DISK	PGM	PROP
UK	PC Security Ltd	Stoplock III	PC	SW	DISK	PGM	PROP
UK	PC Security Ltd.	Stoplock IVE	PC	SW/HW	DISK	PGM	DES
UK	PC Security Ltd.	Stoplock KE	PC	SW	DISK	PGM	PROP
UK	PC Security Ltd.	Stoplock V	PC	SW	DISK	PGM	PROP
UK	PC Security Ltd.	Stoplock V/SC	PC	SW/HW	DISK	SMART CARD	PROP
UK	Plessy Crypto	RSA chip		HW		CHIP	RSA
UK	Plus 5 Engineering Ltd.	Policeman	PC	SW	DISK	PGM	PROP
UK	Portcullis Computer Security Ltd.	Cryptix Toolkit		SW	GENERAL	KIT	DES
UK	Portcullis Computer Security Ltd	Easycrypt		SW			DES
UK	Portcullis Computer Security Ltd.	TRISPAN V.12130	DOS	SW/HW	FILE	<See Notes>	
UK	Protection Systems Ltd.	Disk Certification	PC	SW	DISK	PGM	PROP
UK	Protection Systems Ltd	Guardian Angel LAN	PC	SW	FILE	PGM	PROP
UK	Protection Systems Ltd.	Guardian Angel Plus	PC	SW	FILE	PGM	PROP
UK	Protection Systems Ltd.	Guardian Angel Plus LAN	PC	SW	FILE	PGM	PROP
UK	Racal Airtech Ltd.	Datacryptor 64	RS232	HW	COMMS	BOX	DES
UK	Racal Airtech Ltd.	Datacryptor 64E	X.25	HW	COMMS	BOX	DES
UK	Racal Airtech Ltd.	Datacryptor 64F	RS232	HW	COMMS	BOX	DES
UK	Racal Airtech Ltd.	Datacryptor 64HS	G.703	HW	COMMS	BOX	DES
UK	Racal Airtech Ltd.	Datacryptor 64HSF	RS232	HW	COMMS	BOX	DES
UK	Racal Airtech Ltd.	Datacryptor 64MS	RS232	HW	COMMS	BOX	DES
UK	Racal Airtech Ltd.	Datacryptor&trade 2000	RS232	HW	COMMS	BOX	DES
UK	Racal Airtech Ltd.	RG721 PC Security Module	DOS	SW/HW	GENERAL	ISA	DES
UK	Racal Airtech Ltd.	Safe 64K Link Encryptor	RS232	HW	COMMS	BOX	DES
UK	Racal Airtech Ltd.	Safe Megabit 2 Encryptor		HW	COMMS	BOX	DES
UK	Racal Airtech Ltd.	Safe X.25	WIN	HW	COMMS	BOX	DES
UK	Racal Airtech Ltd.	WatchWorld II Token		HW	PIN	TOKEN	DES

UK	Racal Airtech Ltd.	WatchWorld Soft Token	Win	HW	PIN	DISK	DES
UK	Racal Airtech Ltd.	WebSentry Ethernet (WS-ES)	DOS	SW/HW	SSL	BOX	DES
UK	Radius	??					
UK	Reflex Magnetics Ltd.	Reflex Disknet		HW			
UK	S&S International PLC	Dr. Solomon's Ringfence II	PC	SW	DISK	PGM	PROP
UK	S&S International PLC	SAVEDIR	PC	SW	FILE	PGM	PROP
UK	Secuncor 3net Ltd.	Secure IQ ENCO		HW	COMMS		DES
UK	Sington Associates	??					
UK	Smith's Associates	??					
UK	Soft Concepts	Ncrypt	WIN	SW	FILE	PGM	PROP
UK	Softdiskette	??					
UK	Sophos Ltd.	D-Fence 4 HMG	PC	SW	DISK	PGM	HMG
UK	Sophos Ltd.	D-Fence 4 SPA	PC	SW	DISK	PGM	PROP
UK	Sophos Ltd.	E-DES	DOS	SW	FILE	PGM	DES
UK	Sophos Ltd.	PUBLIC	pc	SW	COMMS	PGM	DES
UK	Straitors Data	PS3					
UK	Sygnus Data Communications	??					
UK	Time & Data Systems	Microstop					
UK	Tricom	??					
UK	University College London	OSISEC Version 2.3		SW	GENERAL	PGM	DES
UK	University College London	UCL-PEM		SW	EMAIL	PGM	DES
UK	Widney Ash	??					
UK	Zeta Communications Ltd.	Zetacoda A	RS232	HW	COMMS	BOX	PROP
UK	Zeta Communications Ltd.	Zetacoda X	RS232	HW	COMMS	BOX	PROP

C. FOREIGN ENCRYPTION MANUFACTURERS AND DISTRIBUTORS BY COUNTRY

The following table is a summary listing of the foreign companies that manufacture or distribute cryptographic products.

COUNTRY	COMPANY
ARGENTINA	Data Crypt S.A.
ARGENTINA	Newnet S.A.
AUSTRALIA	Andrei Souleimanian
AUSTRALIA	Banksia Technology Pty. Ltd.
AUSTRALIA	Carbon Based Software
AUSTRALIA	Cipher Research Laboratories
AUSTRALIA	Cryptsoft Pty Ltd.
AUSTRALIA	Cybanim Pty Ltd.
AUSTRALIA	DataCrypt
AUSTRALIA	Datamatic Pty. Ltd.
AUSTRALIA	Eracom Pty Ltd.
AUSTRALIA	Eric Young
AUSTRALIA	Loadplan Australasia Pty Ltd.
AUSTRALIA	LUCENT
AUSTRALIA	Matthew Kwan
AUSTRALIA	Microlock
AUSTRALIA	Microsoft Pty.
AUSTRALIA	Mosaic Industries
AUSTRALIA	NetSafe
AUSTRALIA	News Datacom
AUSTRALIA	NexSol
AUSTRALIA	Nick Payne
AUSTRALIA	Robust Software
AUSTRALIA	Ross Williams
AUSTRALIA	RSA Data Security Australia
AUSTRALIA	Secure Network Solutions
AUSTRALIA	Security Domain Pty Ltd
AUSTRALIA	TRAC Systems
AUSTRALIA	Tracom
AUSTRIA	Eshelbeck, Steiner, Beitelmair
AUSTRIA	IAIK, TU Graz
AUSTRIA	Mrs Elektronik
AUSTRIA	Siemens AG Austria
AUSTRIA	University of Linz
BAHRAIN	International Information Systems
BALTIC REPUBLICS	LAN Vision
BANGLADESH	Quanium System Software
BELGIUM	ClassicSys
BELGIUM	CNET
BELGIUM	Cryptech NV/SA
BELGIUM	Data Alert International Eithoven BV
BELGIUM	GSA Ran Data Europe
BELGIUM	Highware, Inc.
BELGIUM	Lintel Security
BELGIUM	Open Software Foundation / Europe
BELGIUM	UTI-MACO Belgium
BELGIUM	Vector
BRAZIL	PC Software e Consultoria Ltda
BRUNEI	Digitus Computer Systems
CANADA	A.B. Data Sales, Inc.
CANADA	Adam Berent
CANADA	Atlantic Systems Group (ASG)
CANADA	Authentex/NovaStor
CANADA	Certicom
CANADA	Chrysalis ITS
CANADA	Compression Technologies, Inc.
CANADA	Computer Security Corporation
CANADA	CRYPTOCard Corporation
CANADA	Cycomm International, Inc.
CANADA	Earthworks Communications
CANADA	Entrust Technologies
CANADA	Freestyle Software, Inc.
CANADA	Gandalf
CANADA	Ilex Systems Inc.
CANADA	Intoron Technologies, Inc.
CANADA	Isolation Systems
CANADA	Jaws Technologies, Inc
CANADA	Kyberpass Corporation
CANADA	Micro Tempus, Inc.
CANADA	Microsoft Canada, Inc.
CANADA	Milkyway Networks Corporation
CANADA	MPR Teltech
CANADA	NetComServ Canada
CANADA	Newbridge Networks Corp.
CANADA	Nortel Secure Networks
CANADA	Northern Telecom Canada Ltd. (Data Comm. Products)
CANADA	Northern Telecom Canada Ltd. (Secure Networks)

CANADA	Octothorp Industries
CANADA	Okiok Data
CANADA	Ontrack Computer Systems, Inc.
CANADA	Paradyne Canada Ltd.
CANADA	Queen's University
CANADA	RAYBCRG TECHNOLOGIES INC.
CANADA	Scientific Atlantic
CANADA	Secured Communications Inc. (SCI)
CANADA	Sierra Wireless
CANADA	Skanis Technology
CANADA	Symantec, Canada
CANADA	The Enigma Group
CANADA	TimeStep Corporation
CANADA	Tundra Semiconductor Corp.
CANADA	Xcert International, Inc.
CANADA	Zoomit Corporation
CHILE	Bysupport Computacion SA
COLUMBIA	Economic Data sl
CYPRUS	A.E.C. Consultants Ltd
CZECH REPUBLIC	Alwil Software
CZECH REPUBLIC	Decros spol. s r.o.
CZECH REPUBLIC	PCS spol sro
DENMARK	Aarhus University, Computer Science Department
DENMARK	CryptoMathic A/S
DENMARK	GN Datacom
DENMARK	Intelitech Omniware
DENMARK	Iversen & Martens A/S
DENMARK	Kommunedata
DENMARK	LSI Logic/Dataduo AS
DENMARK	Swanholm Computing A/S
DENMARK	Swanholm Distribution A/S
DENMARK	Telesec
ESTONIA	Cybernetica
FINLAND	Antti Louko
FINLAND	Ascom Fintel OY
FINLAND	Datafellows Ltd
FINLAND	Instrumentoli OY
FINLAND	Jetico, Inc.
FINLAND	LAN Vision OY
FINLAND	SSH Communications Security
FINLAND	SSH Communications Security
FRANCE	AB Soft
FRANCE	ActivCard
FRANCE	Aladdin France SA
FRANCE	Atlantis
FRANCE	Bull Worldwide Information Systems Inc
FRANCE	CCETT
FRANCE	Cryptech France
FRANCE	Crypto-Box Sarl
FRANCE	CSEE - Division Communication et Informatique
FRANCE	CSIL
FRANCE	Dassault Automatismes et Telecommunications
FRANCE	Digital Equipment Corp. (DEC), Paris Research Lab
FRANCE	Herve Schauer Consultants
FRANCE	Hewlett Packard France
FRANCE	Imaga France S.A.R.L
FRANCE	LAAS
FRANCE	Netscape Communications CNIT
FRANCE	Philips Communication Systems
FRANCE	Premenos Europa
FRANCE	Rast Electronics
FRANCE	Research Institute
FRANCE	S.A. Gretag
FRANCE	SAGEM
GERMANY	Andreas Kupries
GERMANY	Andreas Muller Software
GERMANY	AR Datensicherungssysteme GmbH
GERMANY	Atlantis GmbH (deutschland)
GERMANY	Bailer & Huwig
GERMANY	BioData GmbH
GERMANY	BROKAT Infosystems AG
GERMANY	CCI (Competence Center Informatik GmbH)
GERMANY	CE Infosys GmbH
GERMANY	Cedric Reinartz
GERMANY	Cellcon
GERMANY	Christoph Martin
GERMANY	Concord-Eracom Computer GmbH
GERMANY	Controlware GmbH
GERMANY	CryptoSoft GmbH
GERMANY	CryptoSoft GmbH
GERMANY	DataSafe
GERMANY	DemCom
GERMANY	DTM Data TeleMark GmbH
GERMANY	Dynatech - Gesellschaft fur Datenverarbeitung GmbH
GERMANY	EuroCom EDV
GERMANY	EZI GmbH
GERMANY	FAST ComTec GmbH
GERMANY	GAO
GERMANY	Gliss & Herweg
GERMANY	Glück & Kanja GmbH
GERMANY	GMD
GERMANY	Gretag Elektronik GmbH
GERMANY	Interconnect

GERMANY	Jurgen Meyer, Frank Gadegast
GERMANY	Karl Huwig
GERMANY	KryptoKom
GERMANY	Markt & Technik Software Partners Intl. GmbH
GERMANY	MARX Datentechnik GmbH
GERMANY	Mathias Kretschmer
GERMANY	Paradyne GmbH
GERMANY	Roland Mundloch
GERMANY	S&S International Deutschland GmbH
GERMANY	Siemens Vertrauliche Kommunikation
GERMANY	Siemens-Nixdorf
GERMANY	SIT
GERMANY	T. Billenstein
GERMANY	Tela Versicherung
GERMANY	Tele Security Timmann GmbH & Co.
GERMANY	Telenet Kommunikation Systeme
GERMANY	The Compatibility Box GmbH
GERMANY	Toshiba Europe GmbH
GERMANY	Utimaco Safeware AG
GERMANY	Wilhelm Heibl Werke
GHANA	Software Marketing Consultancy
GREECE	A E C Consultancy
GREECE	G.J.Messantis & Co. Ltd.
GREECE	John Ioannidis
GREECE	ORCO Ltd.
HONG KONG	Digitus Computer Systems
HONG KONG	Microsoft Hong Kong, Ltd.
HONG KONG	News Datacom
HONG KONG	ROCTEC Enterprises, Ltd.
HONG KONG	Techtrend Engineering, Ltd. (TEL)
HONG KONG	Triple D Ltd.
ICELAND	Logi Ragnarsson
ICELAND	Softis nf
INDIA	Bharat Electronics Ltd.
INDIA	Chenab Info Technology
INDIA	DCM Data Products
INDIA	Digital Electronics Ltd.
INDIA	Digital Equipment (India) Ltd.
INDIA	Hewlett-Packard (India) Pvt. Ltd.
INDIA	Hinditron Computers Pvt. Ltd.
INDIA	International Computers Indian Manufacture Ltd
INDIA	International Data Management Ltd.
INDIA	OMC Computers Ltd.
INDIA	Palm Computer Systems Ltd., Export Division
INDIA	PSI Data Systems Ltd.
INDIA	Quantum System Software
INDIA	Rolta India Limited
INDIA	Tata Burroughs Ltd.
INDIA	Tata Consultancy Services
INDIA	Tata Unisys Ltd.
INDIA	Texas Instruments (India) Pvt. Ltd.
INDIA	Wipro Systems Limited
INDONESIA	Digitus Computer Systems
IRAN	Communications Industries Group
IRAN	Shabakeh Gostar Corporation
IRELAND	AT&T Network Systems Ireland
IRELAND	Eurologic Systems, Ltd.
IRELAND	Isocor Ireland
IRELAND	Priority Data Systems Ltd
IRELAND	Renaissance Contingency Services Ltd.
IRELAND	Shamus Software Ltd.
IRELAND	Silicon Software Systems Ltd.
IRELAND	Software and Systems Engineering Ltd.
IRELAND	Software Systems Engineering Ltd.
IRELAND	Systemics Ltd.
ISLE OF MAN	Invisimail International Ltd.
ISRAEL	Aladdin Knowledge Systems, Ltd.
ISRAEL	Algorithmic Research Ltd.
ISRAEL	Alroo Ltd.
ISRAEL	Areshelt Systems Ltd.
ISRAEL	Carmel Software Engineering Ltd.
ISRAEL	Check Point Software Technologies Ltd
ISRAEL	Elementrix Technologies Ltd.
ISRAEL	Ins Software
ISRAEL	News Datacom
ISRAEL	RADGUARD, Ltd
ISRAEL	Secure Network Systems, Ltd.
ISRAEL	Tadiran
ISRAEL	Vanguard Security Technologies Ltd.
ITALY	AMTEC SPA
ITALY	CERT-IT
ITALY	Eutron Spa
ITALY	Incaa SRL
ITALY	Olivetti
ITALY	Ratio Srl
ITALY	Sicsistemi an
ITALY	Systems Communicazoni srl
ITALY	TELSY Elettronica e Telecomunicazioni S.p.A.
ITALY	Telvox s.a.s.
IVORY COAST	Software Marketing Consultancy
JAPAN	ADVANCE Co., Ltd.
JAPAN	Compal Inc
JAPAN	Fujitsu Labs Ltd.

CANADA	Octothorp Industries
CANADA	Okiok Data
CANADA	Ontrack Computer Systems, Inc.
CANADA	Paradyne Canada Ltd.
CANADA	Queen's University
CANADA	RAYBORG TECHNOLOGIES INC.
CANADA	Scientific Atlantic
CANADA	Secured Communications Inc. (SCI)
CANADA	Sierra Wireless
CANADA	Silanis Technology
CANADA	Symantec, Canada
CANADA	The Enigma Group
CANADA	TimeStep Corporation
CANADA	Tundra Semiconductor Corp.
CANADA	Xcert International Inc.
CANADA	Zoomit Corporation
CHILE	Bysupport Computacion SA
COLUMBIA	Economic Data sl
CYPRUS	A.E.C. Consultants Ltd
CZECH REPUBLIC	Alwil Software
CZECH REPUBLIC	Decros spol. s r.o.
CZECH REPUBLIC	PCS spol sro
DENMARK	Aarhus University, Computer Science Department
DENMARK	CryptoMathic A/S
DENMARK	GN Datacom
DENMARK	Intellitech Omniware
DENMARK	Iversen & Martens A/S
DENMARK	Kommunedata
DENMARK	LSI Logic/Dataco AS
DENMARK	Swanholm Computing A/S
DENMARK	Swanholm Distribution A/S
DENMARK	Telesec
ESTONIA	Cybernetica
FINLAND	Antti Louko
FINLAND	Ascom Fintel OY
FINLAND	Datafellows Ltd.
FINLAND	Instrumentoli OY
FINLAND	Jetico, Inc.
FINLAND	LAN Vision OY
FINLAND	SSH Communications Security
FINLAND	SSH Communications Security
FRANCE	AB Soft
FRANCE	ActivCard
FRANCE	Aladdin France SA
FRANCE	Atlantis
FRANCE	Bull Worldwide Information Systems Inc.
FRANCE	CCETT
FRANCE	Cryptech France
FRANCE	Crypto-Box Sarl
FRANCE	CSEE - Division Communication et Informatique
FRANCE	CSIL
FRANCE	Dassault Automatismes et Telecommunications
FRANCE	Digital Equipment Corp. (DEC), Paris Research Lab
FRANCE	Herve Schauer Consultants
FRANCE	Hewlett Packard France
FRANCE	Incaa France S.A.R.L.
FRANCE	LAAS
FRANCE	Netscape Communications CNIT
FRANCE	Philips Communication Systems
FRANCE	Premenos Europa
FRANCE	Rast Electronics
FRANCE	Research Institute
FRANCE	S.A. Gretag
FRANCE	SAGEM
GERMANY	Andreas Kupries
GERMANY	Andreas Muller Software
GERMANY	AR Datensicherungssysteme GmbH
GERMANY	Atlantis GmbH (deutschland)
GERMANY	Baller & Huwig
GERMANY	BioData GmbH
GERMANY	BROKAT Infosystems AG
GERMANY	CCI (Competence Center Informatik GmbH)
GERMANY	CE Infosys GmbH
GERMANY	Cedric Reinartz
GERMANY	Celticon
GERMANY	Christoph Martin
GERMANY	Concord-Eracom Computer GmbH
GERMANY	Controlware GmbH
GERMANY	CryptoSoft GmbH
GERMANY	CryptoSoft GmbH
GERMANY	DataSafe
GERMANY	DemCom
GERMANY	DTM Data TeleMark GmbH
GERMANY	Dynatech - Gesellschaft fur Datenverarbeitung GmbH
GERMANY	EuroCom EDV
GERMANY	EZI GmbH
GERMANY	FAST ComTec GmbH
GERMANY	GAO
GERMANY	Gliss & Herweg
GERMANY	Glück & Kanja GmbH
GERMANY	GMD
GERMANY	Gretag Elektronik GmbH
GERMANY	Interconnect

JAPAN	Jade Corporation Ltd
JAPAN	Mitsubishi Electric Corporation
JAPAN	Mitsubishi Electric Engineering Company Ltd
JAPAN	Netscape Communications KK Japan
JAPAN	Nihon RSA
JAPAN	Nipon Telephone & Telegraph
JAPAN	Open Software Foundation / Pacific
JAPAN	Paradyne Japan, KK
JAPAN	Toshiba Information Systems (Japan)
JAPAN	Yokohama National University
KENYA	Memory Masters
KUWAIT	LBI International
LUXEMBOURG	Data Alert International Elfhoven BV
MADAGASCAR	Megabyte Computers
MALAYSIA	Digitus Computer Systems
MALTA	LBI International, Inc.
MALTA	Panta Computer Co Ltd.
MALTA	Shreburn Co. Ltd.
MAURITIUS	Megabyte Computers Ltd.
MEXICO	Computer Security Corporation
MEXICO	Ontrack Computer Systems, Inc
MEXICO	Seguridata Privada S.A. de C.V.
MEXICO	The King of Hearts
NEPAL	Quantum System Software
NETHERLANDS	Ad Infinitum Programs (AIP-NL)
NETHERLANDS	Alco Blom Software
NETHERLANDS	Asot B.V.
NETHERLANDS	Atlantic Nederland BV
NETHERLANDS	Concord Eracom Nederland BV
NETHERLANDS	CRYPSYS Data Security
NETHERLANDS	Cryptech Nederland
NETHERLANDS	Data Alert International Elfhoven BV
NETHERLANDS	DigiCash
NETHERLANDS	DSP International
NETHERLANDS	Elfhoven Automatisering
NETHERLANDS	ElleShim Europe B.V.
NETHERLANDS	Geveke Electronics BV
NETHERLANDS	Incaa Datacom BV
NETHERLANDS	Incaa Nederland B.V.
NETHERLANDS	Philips Crypto B.V.
NETHERLANDS	Pijnenburg
NETHERLANDS	PTT
NETHERLANDS	Symantec, Netherlands
NETHERLANDS	Tulip Computers BV
NETHERLANDS	Verspeck & Soeters b.v
NEW ZEALAND	CES Communications Ltd.
NEW ZEALAND	John Gilmore
NEW ZEALAND	Loadplan Australasia Pty Ltd
NEW ZEALAND	LUC Encryption Technology, Ltd. (LUCENT)
NEW ZEALAND	Microsoft New Zealand
NEW ZEALAND	Peter Gutmann
NEW ZEALAND	RPK New Zealand Ltd
NIGERIA	Software Marketing Consultancy
NORWAY	Alladin Software
NORWAY	BDC Bergen Data Consulting A/S
NORWAY	Bergen Data Consulting A.S.
NORWAY	Columbi Micro a.s.
NORWAY	Ericsson Senator
NORWAY	InfoMedica AS
NORWAY	Informasjonskontroll A/S
NORWAY	Informatikk A/S
NORWAY	Kirkedam Elektronikk EDB
NORWAY	Noris A.S
NORWAY	PDI
NORWAY	Scand PC Sys/Sectra
NORWAY	Siemens Nixdorf, Informasjonssystemer A/S
NORWAY	Skandidek A/S
NORWAY	Sterling Software Scandinavia A/S
NORWAY	Swanholm Distribution A/S
NORWAY	Telepartner as
NORWAY	Voicetech A.S
OMAN	LBI International
PHILIPPINES	Digitus Computer Systems
POLAND	Dagma sp z o o
POLAND	Enigma Information Security Systems
POLAND	SCFT-u.1.
PORTUGAL	Informova
PORTUGAL	Redislogar SA
PORTUGAL	RSVP Consultores Associados Lda
QATAR	LBI International
REUNION	Megabyte Computers
ROMANIA	Interscope s.r.l.
RUSSIA	<UNKNOWN>
RUSSIA	Ancort
RUSSIA	Axon
RUSSIA	Elias Ltd.
RUSSIA	INFORM - RTG
RUSSIA	LAN Crypto
RUSSIA	RESCrypto
RUSSIA	ScanTech
RUSSIA	TELECRYPT, Ltd.
SAUDI ARABIA	Info Guard Saudi Arabia
SAUDI ARABIA	LBI International Ltd

SINGAPORE	Communications Systems Engineering Pty. Ltd.
SINGAPORE	Dietheim Singapore Pte. Ltd
SINGAPORE	Digitus Computer Systems
SINGAPORE	Digitus Computer Systems
SINGAPORE	Microsoft Singapore Pte, Ltd
SLOVAK REPUBLIC	Lynx sro
SLOVAK REPUBLIC	PCS Bratislava sro
SOUTH AFRICA	BSS (Pty) Ltd.
SOUTH AFRICA	BSS (Pty) Ltd.
SOUTH AFRICA	Citadel Data Security
SOUTH AFRICA	Computer Security Associates
SOUTH AFRICA	Denel Informatics
SOUTH AFRICA	EFT
SOUTH AFRICA	Intelligent
SOUTH AFRICA	Nanoteq
SOUTH AFRICA	Net One
SOUTH AFRICA	NetSec
SOUTH AFRICA	Sentera
SOUTH AFRICA	Siemens Ltd. So. Africa -Pretoria
SOUTH AFRICA	Siemens Ltd.-So Africa
SOUTH AFRICA	Spescom
SOUTH AFRICA	Thawte Consulting
SOUTH KOREA	Digitus Computer Systems
SOUTH KOREA	Future Systems, Inc.
SOUTH KOREA	JiranSoft
SOUTH KOREA	Penta Security Systems Inc.
SOUTH KOREA	Senex Technologies Inc. Ltd
SOUTH KOREA	SoftForum
SPAIN	Asociacion Espanola de Empresas de Informatica
SPAIN	Asociacion Nacional de Industrias Electronicas
SPAIN	Atlantis Iberica
SPAIN	Economic Data al
SPAIN	SECARTYS
SPAIN	Sinutec
SWEDEN	Ardy Elektronics
SWEDEN	AU-System Communication AB
SWEDEN	AU-System Infocard AB
SWEDEN	AV System Infocard
SWEDEN	Business Security AB
SWEDEN	COST Computer Security Technologies International
SWEDEN	DynaSoft
SWEDEN	Glenn Larsson
SWEDEN	Henry Padilla
SWEDEN	QA Informatik AB
SWEDEN	SECTRA AB
SWEDEN	SONNOR Crypto AB
SWEDEN	Stig Ostholm
SWITZERLAND	ASCOM Tech AG
SWITZERLAND	Brown-Boveri
SWITZERLAND	Crypto AG
SWITZERLAND	Ete-Hager AG
SWITZERLAND	ETH Zurich
SWITZERLAND	ETH Zurich
SWITZERLAND	Gretacoder Data Systems AG
SWITZERLAND	Incaa Datacom AG
SWITZERLAND	Lightning Instrumentation SA
SWITZERLAND	Markt & Technik Vertnebs AG
SWITZERLAND	Omnisec AG
SWITZERLAND	Organa
SWITZERLAND	Safeware AG
SWITZERLAND	Theissen Security Systems Ltd.
TAIWAN	Digitus Computer Systems
THAILAND	Digitus Computer Systems
TURKEY	ASELSAN Inc.
TURKEY	Logosoft Yazlim San Tic Ltd
UAE	LBI International
UK	<UNKNOWN>
UK	Adam Back
UK	Andrew Brown
UK	Apricot Computers, Ltd.
UK	Atlantic Coast plc.
UK	Avant Guardian Ltd.
UK	Baltimore Technologies plc.
UK	Ben Laurie
UK	British Telecom
UK	Business Simulations
UK	Cambridge Electric Industries
UK	Codepoint Systems Ltd.
UK	Computer Security Ltd.
UK	Cray Electronics Holding, PLC
UK	Cylink Ltd
UK	Data Innovation Ltd.
UK	Datamedia Corporation, Ltd.
UK	DataSoft International Ltd.
UK	Digital Crypto
UK	Dynatech Communications Ltd. (Northern office)
UK	Dynatech Communications Ltd.
UK	Emergent Technologies, Ltd.
UK	EngRus
UK	Ewen Associates Limited
UK	Fauzan Mirza
UK	Finansa
UK	Fulcrum Communications

UK	GEC-Marconi Secure Systems
UK	Gelosia
UK	Gretag Ltd.
UK	Honeywell
UK	ICL Secure Systems
UK	Incaa UK
UK	InfoShare
UK	Instant Access
UK	Interconnections
UK	International Data Security, Ltd.
UK	International Software Management
UK	iQ International
UK	IT Security International
UK	ITV
UK	J.R.Ward Computers Ltd.
UK	J.S.A. Kapp
UK	Jaguar Communications Ltd.
UK	Janus Sovereign
UK	JCP Computer Services
UK	JPY Associates Ltd.
UK	Loadplan
UK	Logica
UK	Microfi Technology Ltd.
UK	Microsoft Ltd.
UK	NEST Ltd.
UK	Network Systems Corporation (UK)
UK	Newbridge Networks Ltd
UK	News Datacom
UK	Northern Telecom Europe Ltd.
UK	Novell, Ltd. (UK)
UK	Paradyne European Headquarters
UK	PC Security Ltd.
UK	Plessy Crypto
UK	Plus 5 Engineering Ltd.
UK	Portcullis Computer Security Ltd.
UK	PPCP
UK	Premenos UK Limited
UK	Prosoft Ltd.
UK	Protection Systems Ltd.
UK	Racal Air Tech
UK	Racal Airtech Ltd.
UK	Radius
UK	Reflex Magnetics Ltd
UK	S&S International PLC
UK	Sapher Servers Ltd.
UK	Secuncor 3net Ltd.
UK	Sington Associates
UK	SmartDisk Security Corp. UK (SDSC)
UK	Smith's Associates
UK	Soft Concepts
UK	Softdiskette
UK	Sophos Ltd
UK	Strafford Data
UK	Sygnus Data Communications
UK	Time & Data Systems
UK	Tricom
UK	University College London
UK	Widney Ash
UK	Zeta Communications Ltd.
VENEZUELA	GDV Sistemas
WEST INDIES	Global Traders Inc Ltd
WEST INDIES	Global Traders Inc Ltd
YUGOSLAVIA	Sophos Yu d.o.o.
ZIMBABWE	RyVal Computer (Prvate) Ltd

D. REPORT OF THE PRESIDENT'S EXPORT COUNCIL SUBCOMMITTEE ON ENCRYPTION, WORKING GROUP ON INTERNATIONAL ISSUES

The following findings have been adopted by the PECSENC as a reflection of conditions of international competition prior to the U.S. Government's liberalization of encryption export controls announced on September 16, 1998. The liberalization may affect many of these findings, and the findings will be used as a baseline for a review of the effects of the liberalization in future sessions of the PECSENC.

1. The difference between U.S. encryption controls and those of other nations is a serious—but not the only—factor determining success in the computer security

market. With or without controls, both U.S. and foreign products are likely to continue to coexist, and other factors are likely to continue to slow deployment of security products. Many foreign companies, for example, especially those influenced by governments, will continue to favor domestic security solutions, and many computer users will not deploy serious security technology until there have been major incidents with losses that can be attributed to lack of encryption.

2. Nonetheless, the adverse impact of controls on U.S. industry is palpable. For many software applications, business customers simply demand security and encryption; it is a checklist item, and its absence is a deal breaker. While simply counting the number of foreign encryption software products in the market is not an accurate measure of the impact of controls, one particularly serious risk is that non-U.S. companies will use their ability to export stronger encryption as "leverage" to dominate particular applications.

This has happened in at least one field—Internet banking—and may occur in other areas of electronic commerce. Brokat, a German company that scarcely existed four years ago, now has 250 employees and offices in several countries including the United States. Brokat's specialty is Internet banking and electronic commerce, but it broke into that business on the strength of being able to offer stronger encryption than German banks could obtain in Netscape or Microsoft browsers. It is now a major player in this niche, with 50% of the European Internet banking market and enough U.S. customers to justify a 20-person U.S. branch office. Meanwhile, encryption constitutes 10% or less of Brokat's revenue, and it has expanded its initial Internet banking offerings to include support for other forms of electronic commerce. Loss of U.S. competitiveness in the electronic commerce software market obviously raises concerns not just about encryption software but other software opportunities. Indeed, it foreshadows a weakening of the U.S. position as a leader in electronic commerce generally.

3. The persistent emphasis in U.S. export control policy over the past two years on key recovery, or "lawful access," has also taken a toll on the credibility of U.S. security products. Key recovery continues to find a market. Business wants to ensure that data are available for corporate purposes, including litigation. Key recovery is seen as an important feature for stored business data (though not for communicated data in transit).

But the use of export controls to drive the key recovery market further than it would go by itself is hurting U.S. industry. Foreign governments and competitors, particularly in Europe, have misinterpreted this U.S. policy, perhaps deliberately. In essence, foreign customers are told often by their governments as well as local security companies that all U.S. encryption products come with a back door allowing the U.S. government to read the contents. In part this is the result of outmoded "Recovery" supplements to U.S. export rules that demand an unrealistic level of U.S. government access to key recovery products. In part it reflects the hostility of many foreign governments toward U.S. key recovery and access policies. It also reflects the fact that some countries will simply never rely on security products that are not home-grown, and misunderstanding U.S. key recovery policies may simply be a handy stick to beat U.S. products with. But it is unfortunate that the U.S. government has provided such a large and easily wielded stick.

4. U.S. controls are driving many U.S. companies into "cooperative arrangements" with foreign encryption suppliers. These cooperative arrangements allow U.S. companies to provide complete security solutions by encouraging their foreign partners to marry foreign-made crypto with U.S. commercial applications. These cooperative arrangements are highly risky under U.S. Iaw, but they are not unlawful per se. Given the stakes, many companies have been prepared to take risks under U.S. law, and it is expected that more will do the same. The result is that U.S. policy has fostered the development of cryptographic software and hardware skills outside the United States. German, Swiss, Canadian, Russian, and Israeli cryptography companies have all benefited from this unintended consequence of U.S. encryption policy.

5. The U.S. government has made efforts to "level the field" of disparate export controls for encryption through negotiations under the Wassenaar Agreement. The U.S. proposal that 56-bit encryption become a new "floor" for encryption exports under Wassenaar, while certainly better than current policy, is likely to be implemented at least a year and perhaps several years too late. In response to the U.S. KMI initiative, which conditionally decontrolled 56-bit encryption in December 1996, other countries also decontrolled 56-bit DES but more or less unconditionally. The countries include Canada and apparently the United Kingdom. And by 1996, other countries, such as Germany, already were approving the export of 56-bit DES to virtually any country for virtually any purpose. Most recently, the exhaustion of a 56-bit DES key using a machine built for a quarter million dollars has entirely discredited DES as a serious security tool for valuable secrets. Single DES remains a useful

tool for assuring privacy against a wide variety of potential adversaries and snoops, but decontrolling 56-bit encryption will not provide a significant boost to the competitiveness of U.S. technology for serious security applications.

6. Process and timing: In 1995, the State Department approved routine license applications for the export of encryption in less than a week on average. This was when the State Department had jurisdiction over encryption and NSA staffed the State Department's office and handled all encryption license applications.

This is no longer the case. The Commerce Department has staffed up heavily in the encryption field, but its processes now include parallel reviews by the FBI and NSA under a 30-day deadline that can be extended further with a simple "no" vote by either agency. For whatever reason, these agencies are now taking the full 30 days—and often 90 days. Against a backdrop of continued export liberalization over the past four years, this degradation in export control performance strikes a jarring note.

The Commerce Department's performance in this area is not necessarily out of line with the performance of other countries. The German government often takes two to three months to approve a license for a new product and six weeks to approve a license for routine shipments. The difference is that German companies know with certainty that a license will be issued at the end of the process; and the German government imposes no key recovery requirement on exporters. Therefore, they can make commitments to deliver products that require a license even before they get the license. In the United States, both the FBI and NSA have at times cast votes intended to roll back existing policies, and they have at a minimum managed to stall licenses that seemed to fit existing policy. A key recovery policy, for example, has been applied sporadically to U.S. multinationals and with some inconsistency to other exports. For this reason, it is not prudent for exporters to assume that a license will be issued or to make commitments on the assumption that the license will be issued—even when existing policy makes it seem likely that a license will eventually be granted. Because an RFP by a foreign company may provide only 30 days for responsive proposals, and the proposals often must include an assurance that an export license will be obtained, some U.S. companies lose bidding opportunities simply because the U.S. government does not process licenses quickly enough.

In other respects, of course, Commerce Department practice is a large improvement over State's performance. This is particularly true for controversial licenses, on which Commerce typically forces a decision over a course of months. In contrast, State Department licenses could be held up for months without any explanation and there were no deadlines for resolving interagency disputes. Nonetheless, it seems clear that the Commerce Department and the other participants in the encryption licensing process should adopt additional procedures to speed the granting of relatively non-controversial licenses.

Senator FRIST. Thank you very much, Mr. Hoffman.

Let me begin with Mr. Bidzos. You mentioned that the Administration probably underestimates—you did not say "probably"—underestimates companies overseas, and you mentioned the 3-year delay. Could you comment on both of those?

Mr. BIDZOS. Yes, Mr. Chairman, I would be happy to. When I testified almost 10 years ago I was predicting that we would do economic harm to ourselves if we continued to control encryption, and that turned out to be true. It took 9 years for us to really see it. In fact, we warned at the time that by the time we could point to the damage—because the Administration was saying, "Show us where the harm is, show us how you are being hurt," and my response was: "By the time I can show you lost market share, it is probably too late for you to help me get it back at that point."

So let me now again, 9 years later, look out 3 years and see what might happen. First of all, I think the Administration underestimates the extent to which foreign competitors wish to emulate us. Look at the role that information technology plays in the growth of the U.S. economy. It is absolutely the driving force. It is the engine that is driving unprecedented economic growth, unprecedented in history. The amount of jobs created, the amount of revenue gen-

erated, the amount of innovation, the absolute dollars involved are absolutely unprecedented.

Our foreign competitors are quite aware of this. They are starting to tap public markets for funds to grow. They are starting to target opportunities created by U.S. export policy. Two quick examples of how they are doing that and what the stakes involved are.

First of all, they are actually starting to identify larger products of which encryption is a critical feature and they are starting to build products of those types. They are seeing an opportunity not only to get the encryption revenue, but to get 2, 3, 10, or 20 times the encryption revenues by making a complete product sale.

They also, of course, just by virtue of coming into business as an encryption company because of the opportunity created by U.S. export law, exist and therefore they are able to take advantage of opportunities that they see. If not for export law, they would not even exist.

There is a company in Germany called Brokat which now employs over a thousand people, has raised money in the public market with a very successful public offering, would not exist if it were not for the opportunities created by U.S. crypto.

To go directly to your question, the 3-year timeframe before we can export encryption as strong as the AES, well, first of all, everybody knows that 3 years today is like 15 years was 10 years ago. We live in the Internet age and things happen very, very quickly. Three years is a lifetime. Those companies will exploit opportunities in ways that I mentioned and in other ways that we cannot imagine.

But the real price that we will pay is this. They essentially—it is not a national information infrastructure we are talking about, as the Vice President used to call it. It is a global information infrastructure, there is no question whatsoever. If you look in today's papers, you will conclude very quickly that around the clock global trading of securities is just around the corner. That is not going to happen without a secure information infrastructure and that information infrastructure will be secured, it will be global. The only question is who is going to build it.

The way things sit today, U.S. companies will not build it. U.S. companies will not play the role in building it that they might play.

So these infrastructures that get built are I think critically important in ways we cannot appreciate right now. The company that gets in and builds the infrastructure will have the inside track in selling products and services for 2, 5, 10, and maybe even 20 years down the road because of that early position they stake out for themselves as the infrastructure provider. They set the standards, they have the relationship, etcetera, etcetera.

So this 3 years I am afraid is going to cost us tremendously.

Senator FRIST. In S. 798 we streamline the procedure for receiving an export license by putting a maximum number of days in each step, and you argue that is not enough. Are you arguing for an alternative or are you saying that there should not be these export control policies?

Mr. BIDZOS. Well, maybe I can answer that question by referring to something that Secretary Reinsch said. Secretary Reinsch compared encryption in one respect to supercomputers, machine tools,

biotech, and said that if foreign availability were the sole criteria we would have no export controls on all of those other products. I would submit that encryption does not belong in that category.

If you want to build a supercomputer, if you want to build one and build a lot of them in particular, you need to have incredibly sophisticated technology to manufacture these computers. It is incredibly expensive. You need people with tremendous specialized skills. Just building the systems that can cool the operating supercomputer is incredibly sophisticated. The same is true of manufacturing machine tools. The same thing is true of biotech. You need sophisticated technology just to build the laboratories, the tools, the instruments.

For encryption all you need is a high school textbook and a personal computer. I guess you need Internet access, too, so that brings it down to about 100 million people who are probably capable of doing it. All you need to get into business and duplicate and sell that software is a web site. That may bring it down to 80 million, but it does not get much smaller than that.

You have got companies in South Africa, in Estonia and other places who advertise the fact that they can simply ship you strong encryption that is not subject to U.S. export controls. So we are really in a different situation, where the technology is available and we are not competitive.

Senator FRIST. Thank you.

Professor Hoffman, you have been studying the growth of foreign encryption products for a long time and I appreciate your work very much and your written testimony as well. Do you believe that U.S. export controls have been effective in controlling the development of encryption overseas?

Dr. HOFFMAN. Well, I think you can see from the results of our survey they have been, I would say, marginally effective. They have had some effect, but I think overall the market has had more effect than the U.S. legislation.

Senator FRIST. Mr. Aucsmith, do you have comments on anything that has been said?

Mr. AUCSMITH. I would make one slight addition to Jim's statement about our 3-year window. That has two parts to it. One thing is that the international Internet as we now know it exists because there are international standards. That is what allows everything to work together. It is the glue that holds things together. At this time there are two particular standards being defined worldwide that deal with the security.

IPsec, the Internet Protocol Security Standard, the very thing that will secure point to point connections on the Internet, is being finalized, and already there are many, many countries producing technology that will go into that. If my company and others in the United States cannot participate for 3 years, we will be locked out forever. It is that simple.

The second is, and this is particular to hardware, while we might think we move at an Internet speed, our development cycles mean that there is a long lead time on the piece of hardware, but in the microprocessor area I am working on a microprocessor design that you will not see until the year 2003. I have to make a billion dollar bet today on whether or not I can export that in 2003. It is very,

very hard without some assurance of what the world will look like in terms of legislation at that particular time.

So we will be held out. Every day that this is delayed is a day that we miss products a long time from now.

Senator FRIST. Mr. Aucsmith, could you comment on who should be the trusted parties for recoverable, key recoverable products?

Mr. AUCSMITH. Actually, as I stated before, I am not in favor of key recoverable products, for two primary reasons. One is I think that they fundamentally will not work well, for communications products I do not think that there is any market for that. There is no market need. One could be created artificially by government regulation, but there is no market need.

For stored data, I think the majority of data—in order to be of any use, information has to be shared. It is a rare commodity in information that is valuable and not shared, meaning that if the proverbial person is hit by a bus it is unlikely that he or she is the only one that has access to that information. In fact, in most corporations mission-critical information is stored on databases and is kept in separate mechanisms that have separate access control. I submit that corporations have been dealing with this for quite some time already.

So I would say that in general there should not be trusted third parties, at least not for the key recovery or access control point of view.

Senator FRIST. Mr. Bidzos, could you tell me a bit more, the committee a bit more, about the Internet standards in setting security requirements? Is the 128-bit encryption now the norm?

Mr. BIDZOS. Yes, it is, Mr. Chairman. There is absolutely no question about that. In fact, both in and outside the United States that is the case. Now, I know some of the other witnesses said that it is not used quite as widely as you might be led to believe. I think certainly in the past we have been guilty, as people in industry, of trying to look out into the future and saying, well, this is what is going to happen to us if these export control policies do not change and, sure, maybe we have tended to sort of look at the worst case scenario or closer to that maybe than the middle. But I think the Administration is guilty of some of the same.

Let me give you a couple of specific examples. If you want to bank online with Wells Fargo in California or if you want to access your mutual fund account at Fidelity or any other of scores of financial services institutions, if you want to buy or sell stock online with E-trade, your browser must have 128-bit encryption or you cannot do it. Their servers are configured such that nothing but a browser enabled at 128 bits will work at all.

So even in cases where some people are using the "exportable" lower key lengths in some of these browsers, the primary reason they are doing it is because they are not aware that they are doing it and they have not upgraded. But as soon as they try to use one of these services, they find out that they need to upgrade. This is in the United States. Only under certain conditions can those be sold outside the United States.

So the standards that David alluded to are being developed. They are global standards. The participants in the standards-making process are from all over the world. And David is absolutely right

that companies outside the United States are rapidly moving to build products that comply with those standards and, as we heard from the earlier panel, those foreign competitors of ours will be able to sell worldwide, including in the United States, and we will not. And that is a competitive disadvantage that we will find it very difficult to live with and that we will probably never recover from if we have to wait 3 years.

Senator FRIST. With key length clearly being a moving target even in one hearing, but also as we project ahead, and you are developing products for 3 years from now, and we know that technology is going to progress much faster and that is sort of the theme of this morning, we have advocates for the 128-bit encryption products rather than 64-bit products. How do you propose that we deal with these technological changes legislatively so that we do not have obsolete legislation within 6 months of the time we pass it, recognizing the changes that are under way?

Anybody on the panel? Mr. Aucsmith.

Mr. AUCSMITH. There is a fallacy in trying to regulate technological advancement in general. If you tie it to specific technologies—and in this case, tieing it to specific bit lengths I think it is tieing it to specific technologies. We cannot anticipate necessarily what the market will want 3 years from now in terms of bit length. I would submit that the best way to deal with this in a legislative point of view is to deal with the effects of the technology rather than the technology itself, because I think there is a treadmill that you could get on, having to revisit this very issue every 3 years, which I do not think would be productive for anyone involved. I think if you have it welded to some specific value or some specific technology or specific implementation, you are rife with that.

Dr. HOFFMAN. Mr. Chairman, I agree with the previous witness. It is ill-advised to legislate using bit length only or even some other technological mechanisms. What we have seen in the last several years on this is people focusing on specific things like bit length and avoiding the inevitable, which is what is going to happen when we do have, if you will, ubiquitous, strong, secure encryption. What kind of world is it going to be, how are we going to operate?

We have seen a lot of government resources devoted towards this battle, rather than towards looking at the future and trying to shape it in a more reasonable way.

Senator FRIST. Could you, any of the panelists, comment on what efforts are being made by industry to address the law enforcement agencies' security concerns and develop viable schemes? What is being done? Where are we today? Mr. Aucsmith?

Mr. AUCSMITH. Obviously, the majority of industry is extremely sensitive to the realities of both law enforcement and national security issues. I would submit that I am personally scared of what the future could hold. I think we all should be along those lines.

What we are doing to try to prevent a disaster, if you will, is if you believe that there is an inevitability of this technology being available and its widespread use is inevitable and I think that is about the main point that we tend to disagree with the Government on, is the speed and inevitability, if you will, of that happening the only way to deal with this issue is for a very close co-

operation between the industry that is creating the change and innovating the change and the law enforcement and intelligence communities that need to be able to on occasion use that change to their advantage.

I think things like the national technical center for FBI's competency, I think that is exactly the correct step in the right direction. I think closer cooperation between industry and the Government in terms of assessing vulnerabilities and assessing strengths and weaknesses of various technologies I think is also part of that.

If you will, no commercial product will ever be 100 percent secure because it is not really economically feasible for us to squeeze that last couple of percent out of it. So there will always be vulnerabilities in almost anything that is put out there. Currently those vulnerabilities are exploited by what we would call hackers, if you will, to coin from recent movies, the dark side. What we should be able to do as a government and as responsible industry is, if you will, make the Government the better hackers. It is relatively that simple.

Senator FRIST. Comments, Mr. Bidzos?

Mr. BIDZOS. Yes, Mr. Chairman. Thank you. Well, I guess part of the problem is I think that industry has sort of been busy actively rebuffing a lot of proposals from government over the last dozen years. For example, in 1993 the so-called "Clipper Chip," the first government solution to government access—take my product, embed it in all the products that you build, and that will give me the access—was rebuffed. It just was not something anybody wanted to use.

Later came key recovery and I think government again failed to realize how industry would view key recovery. One simple analogy I can offer you from some of my experience in talking to people in the end user community in large end user organizations, financial companies. One of them described it very well to me, why they objected to some sort of government access to keys.

They said: "Well, darn it, the Government just does not understand how things work out here." They said: "Look, if we are involved in some sort of litigation or some other form of legal dispute, perhaps even being sued by the Government, some sort of antitrust action for example, in all these cases the way the drill works is as follows: A subpoena is delivered, our lawyers review it, and we produce the documents that comply with the request."

We do not give them a key and say: "Look, the documents are stored in that building; here is the key; find what you need and take it, and we will see you later." Essentially, that is how they viewed the proposal for government access to encryption keys, and I think that analogy actually holds up very well.

So you can understand why people resisted it. People do not give some third party a copy of all of the physical keys to their facilities. They have some small organization, a security organization, inside their own company that manages that.

So again, some close cooperation I think would go a long way towards easing, bridging the gap. However, if, as is currently happening, all of the people developing this technology happen to be located in Israel, Singapore, Japan, Ireland, and Germany, it is going to be pretty tough for the U.S. Government to interact with

them and learn and understand and develop products that meet the needs of worldwide industry and certainly U.S. industry.

I think that helps. To me that sort of indicates one of the problems with the current policy. It is gambling heavily.

I do not have a security clearance and I do not know what it was that Director McNamara might have been referring to when she said she would offer some testimony about the threats of ubiquitous encryption, she would offer that in a closed session. But after this many years in the business and spending a lot of time with people who are in that part of it—in fact, I have often awaken at night having dreamed that I was served with a clearance for some of the things I have probably heard I should not have—I think it is fair to say that more than likely it comes down to ubiquitous encryption increasing the cost and complexity of intelligence gathering.

What we have to weigh against that additional cost is the cost to industry in the future. I think for the first time certainly since I have been in this business for 14 years, we are starting to actually be able to see and identify and quantify some of the costs to us of maintaining the current policies.

So hopefully we can strike that better balance. I think the PROTECT Act with some additional amendments would strike a far better balance than we have now.

Senator FRIST. Thank you.

Clearly, today's discussion centers on the security of our Nation, the wellbeing of our Nation, and it is clear that we cannot bind the hands of our American businesses in this new economy that we have all seen really flourish over the last 10, 15, 20 years, and especially over the last 3 to 4 years. We need to make sure that we can compete nationally, internationally. Otherwise we will surrender our global leadership position.

As Federal lawmakers and policymakers, we need to be proactive and we need to be educated, and thus I thank all of our panelists today for participating in that process in this complex policy debate.

A number of my colleagues, the chairman and Senator Burns and Kerry and Abraham and Wyden and a number of others, have worked very hard, and I thank them for their dedication to an issue that is incredibly important to business, to security, and to the national interest.

I want to thank this final panel today, as well as the panels earlier. We will continue to work with you on this very complex but very important policy debate.

With that, we stand adjourned.

[Whereupon, at 11:45 a.m., the committee was adjourned.]

○