AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

THE SECURITY AND FREEDOM THROUGH ENCRYPTION (SAFE) ACT

HEARING

BEFORE THE

SUBCOMMITTEE ON TELECOMMUNICATIONS, TRADE, AND CONSUMER PROTECTION

OF THE

COMMITTEE ON COMMERCE HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

FIRST SESSION

ON

H.R. 850

MAY 25, 1999

Serial No. 106–28

Printed for the use of the Committee on Commerce



U.S. GOVERNMENT PRINTING OFFICE
57–448CC WASHINGTON : 1999

COMMITTEE ON COMMERCE

TOM BLILEY, Virginia, *Chairman*

W.J. "BILLY" TAUZIN, Louisiana
MICHAEL G. OXLEY, Ohio
MICHAEL BILIRAKIS, Florida
JOE BARTON, Texas
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
Vice Chairman
JAMES C. GREENWOOD, Pennsylvania
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
STEVE LARGENT, Oklahoma
RICHARD BURR, North Carolina
BRIAN P. BILBRAY, California
ED WHITFIELD, Kentucky
GREG GANSKE, Iowa
CHARLIE NORWOOD, Georgia
TOM A. COBURN, Oklahoma
RICK LAZIO, New York
BARBARA CUBIN, Wyoming
JAMES E. ROGAN, California
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
ED BRYANT, Tennessee
ROBERT L. EHRLICH, Jr., Maryland

JOHN D. DINGELL, Michigan
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RALPH M. HALL, Texas
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, Jr., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
RON KLINK, Pennsylvania
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
THOMAS C. SAWYER, Ohio
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
KAREN MCCARTHY, Missouri
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
THOMAS M. BARRETT, Wisconsin
BILL LUTHER, Minnesota
LOIS CAPPS, California

JAMES E. DERDERIAN, *Chief of Staff*
JAMES D. BARNETTE, *General Counsel*
REID P.F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON TELECOMMUNICATIONS, TRADE, AND CONSUMER PROTECTION

W.J. "BILLY" TAUZIN, Louisiana, *Chairman*

MICHAEL G. OXLEY, Ohio,
Vice Chairman
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
STEVE LARGENT, Oklahoma
BARBARA CUBIN, Wyoming
JAMES E. ROGAN, California
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
CHARLES W. "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
ROBERT L. EHRLICH, Jr., Maryland
TOM BLILEY, Virginia,
(Ex Officio)

EDWARD J. MARKEY, Massachusetts
RICK BOUCHER, Virginia
BART GORDON, Tennessee
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
ALBERT R. WYNN, Maryland
BILL LUTHER, Minnesota
RON KLINK, Pennsylvania
THOMAS C. SAWYER, Ohio
GENE GREEN, Texas
KAREN MCCARTHY, Missouri
JOHN D. DINGELL, Michigan,
(Ex Officio)

CONTENTS

Page

Testimony of:
- Arnold, Thomas, Vice President and Chief Technology Officer, Cybersource Corporation 41
- Dawson, David D., Chairman and CEO, V-One Corporation 58
- Gillespie, Ed, Executive Director, Americans for Computer Privacy 21
- Holahan, Paddy, Executive Vice President, Marketing, Baltimore Technologies, International Finance Services Centre 54
- Hornstein, Richard, General Counsel, Network Associates, Inc 31
- Lee, Hon. Ronald D., Associate Deputy Attorney General, Department of Justice 17
- McNamara, Hon. Barbara A., Deputy Director, National Security Agency 27
- Reinsch, Hon. William A., Under Secretary of Commerce for Export Administration, Department of Commerce 11
- Schultz, E. Eugene, Trusted Security Advisor, Global Integrity Corporation 47

Material submitted for the record by:
- Goodlatte, Hon. Bob, a Representative in Congress from the State of Virginia, prepared statement of 88
- Schultz, E. Eugene, Trusted Security Advisor and Research Director, Global Integrity Corporation, letter dated June 1, 1999, to Hon. W.J. Tauzin, enclosing response for the record 89

THE SECURITY AND FREEDOM THROUGH ENCRYPTION (SAFE) ACT

TUESDAY, MAY 25, 1999

HOUSE OF REPRESENTATIVES,
COMMITTEE ON COMMERCE,
SUBCOMMITTEE ON TELECOMMUNICATIONS,
TRADE, AND CONSUMER PROTECTION
Washington, DC.

The subcommittee met, pursuant to notice, at 10 a.m., in room 2322, Rayburn House Office Building, Hon. W.J. "Billy" Tauzin (chairman) presiding.

Members present: Representatives Tauzin, Oxley, Stearns, Gillmor, Deal, Largent, Cubin, Rogan, Shimkus, Ehrlich, Bliley (ex officio); Markey, Eshoo, Wynn, Luther, Sawyer, McCarthy, and Dingell (ex officio).

Staff present: Mike O'Rielly, majority professional staff; Cliff Riccio, legislative clerk; and Andy Levin, minority counsel.

Mr. TAUZIN. The hearing will please come to order.

Let me welcome you again. We have assembled a very large but extraordinarily intelligent and informed panel for our subcommittee as we begin thinking in advance about how, in fact, to enter the world of or—rather, the world will be more and more in a digital, highly encrypted age.

We have learned over the past few years that encryption can play an integral role in the development of the digital economy. Individual consumers are looking for certainty and trust when they operate on-line. Our business community wants to integrate encryption into their products and into their daily practices. They also want an opportunity to foil the hacker, the spy, the crook, or competing company before it is too late. Encryption is becoming the modern day door lock. It literally is the dead bolt of the next millennium.

Unfortunately, for all the benefits in encryption, there is a downside. For every legitimate company and person that uses an encryption product, there is a good chance that product can be used for illegal purposes as well. As complex, as mathematically dynamic as they become, encryption products do not discriminate. They treat each user the same, protect each bit of information the same. Thus, the encryption product used to protect the transfer of the new fashion designs from Milan to New York can also be used by terrorists to protect plans for the next attack on innocent civilians.

The Clinton administration and previous administrations before it have treated encryption products guardedly. They see the poten-

tially harmful effects of encryption products and want to keep these products from being used without proper caution or proper approval. To be more accurate, the administration's encryption policy reflects diverging purposes. On the one hand, the administration, led by the intelligence community, wants to contain encryption products from being used abroad more often and interfering with their ability to conduct intelligence gathering. On the other hand, the law enforcement community wants to manipulate the design of encryption products to ensure they can obtain access to the encrypted material as needed with proper authorization.

The current policy, based on good and proper intentions, is a failure. I believe that it is impossible to contain the use of encryption products. In fact, the only encryption products that we are containing are American products from being used internationally.

The world economy is now interdependent. The digital economy is even more dependent on interacting, communicating and conducting business globally. Instead of recognizing this fact, our containment strategy has put ankle-bracelets on American companies. We expect them to thrive and compete, but we put a roadblock in their way. I am glad to see we have a foreign encryption producer here today to talk about international treatment of encryption and how their business is going.

The law enforcement community makes a stronger case for their position, but it, too, does not survive scrutiny. If there was successful, U.S. encryption products would dominate the world, and they would contain a vital component that allows for the decryption of sensitive material on command of a court order. In their view, the faster acceptable American encryption products are created and used, the better.

Unfortunately, this position ignores some very simple facts: the back-door or recoverable mechanisms cannot be forced on current encryption manufacturers. In some market segments, recoverable products could be successful; in others, it will not. In the meantime, the benefits of encryption are delayed or prevented from reaching the needed user. Our law enforcement community cannot force foreign producers in fact to build recoverable products.

I am reminded of an analogy told by a high-technology company on the subject of encryption. When asked whether they could build recoverable products, he said this was like you asking the creators of the atomic bomb to develop a mechanism to put the world back together if it turns out that it shouldn't have been detonated, or it is like asking a farmer to put the egg back together after it has been cooked, eaten and digested.

So I come from the perspective that there are two truths about the debate over encryption products: One, we are unsuccessfully hamstringing U.S. encryption producers and those that want to incorporate encryption into their products based on false pretenses; and, two, the only way that current policy is going to change is for Congress to take action.

The administration likes to play both sides of the issue, and when it looks as though the political pressure is too hot, they make slight changes to the policy. They modified their policy late last year to provide relief for certain market segments, but what happens if you are not in one of those targeted segments? The simple

answer is, you are out of luck; and this is no longer acceptable. That is why I am a supporter and cosponsor of H.R. 850.

H.R. 850 would relax current restrictions to permit export of encryption of any strength without being recoverable. I would be remiss if I didn't point out that while H.R. 850 is a step in the right direction, the bill is missing certain concepts. The Commerce Committee did a great job, I think, on the development of an encryption high-tech laboratory to promote cooperation and the sharing of knowledge between law enforcement and the encryption-producing community. It is our hope that this concept will be continued.

In addition, encryption products have the ability to protect and secure today's communications network, the telecommunications network and the Internet, in ways that are necessary, especially as the dependency of these networks on foreign networks increases. With our jurisdiction over commerce generally, and our expertise on communications policy specifically, I hope we will take the necessary time to improve this bill before us to reflect this aspect of the debate.

I should add, parenthetically, as you know, the Ninth Circuit has entered into this debate. The Ninth Circuit has generally declared the export ban on encryption products to be unconstitutional on the theory that encryption is, in fact, a part of free speech, that without encrypted products, our free speech in this country and around the world would not adequately be protected as the Constitution envisioned.

In that regard, the administration faces the prospect of a decision on whether to appeal that decision. I will be joining with a number of members in a letter to the administration urging them not to appeal the Ninth Circuit decision, rather, to work with us in this committee and in this Congress to pass H.R. 850 with, as I said, with the work of this committee perfecting it in the process; and I would urge other members to consider joining me in that request to the administration to join us in this legislative effort, rather than to pursue a long and extended appeal of the Ninth Circuit decision to the Supreme Court.

I look forward to hearing the witnesses and recognize now the ranking minority member from Massachusetts, my good friend, Mr. Markey.

Mr. MARKEY. Thank you, Mr. Chairman. Thank you so much for having this hearing today.

This issue is a very difficult one from a public policy perspective. Policymakers are asked to balance personal security and freedom with national security and freedom to enable better privacy protection but to also help law enforcement fight crime and to simultaneously salute our clear, economic interests in promoting commercial exporting opportunities of encrypted products and services. During committee deliberations on this encryption legislation in the last session of Congress, I successfully offered an amendment that tried to strike a balance.

There is no member of this committee who is unsympathetic to the plight of law enforcement during this time of profound and rapid technological change. There is no member of this committee who is unwilling to place certain restrictions on the most highly so-

phisticated encryption that would pose national security risks. The problem is that our export controls today have not fully kept up with advances in technology or with the general availability of that technology in commercial products.

Last session I suggested that in headlong pursuit of trying to help law enforcement officials fight crime we ought not rush into adopting rules, regulations or instigating government intrusion into the high-tech marketplace unless we are sure that the proposed solution solves the problem.

I remain convinced that proposals from the law enforcement community need additional work and further analysis. I understand their frustration; and, last session, my amendment tried to get law enforcement the additional tools they need to fight crime. I suggested that the high-tech industry should assist law enforcement and create a national electronic technologies center, a net center, to serve local, State, and Federal law enforcement authorities by providing information and assistance regarding the encryption technologies and techniques.

I still believe that this initiative is preferable to a policy that would place for the first time controls on the domestic use of encryption by American citizens and thereby mandate how every American citizen protects his or her electronic security. I pledge to continue to try to work with the national security and law enforcement communities in trying to fashion a common-sense encryption policy.

The high-tech industry has been highly organized in its effort to liberalize and update U.S. policy toward the export of encryption software and related policies. It has correctly identified the commercial imperative by opening up opportunities for U.S. companies to compete overseas in these critical, knowledge-based industries.

The industry has also been quick to point out that strong encryption can help thwart crime. Moreover, the high-tech industry has noted that strong encryption can also avail customers of greater privacy protection; and the industry has been eager to assist consumers by creating products that permit people to safeguard their personal conversations or data files.

For all of these efforts, I wholeheartedly commend the high-tech industry. I only wish that the industry would be equally zealous in protecting the privacies of consumers when its commercial interests are more complicated, whether it is the Intel Pentium III chip or unique identifiers in Windows software or E-commerce products yet to come. With respect to transactional on-line privacy, the industry has been less attentive to balancing security interests with personal privacy while consumers are on-line.

A recent survey conducted by the Georgetown Business School of on-line websites found that upwards of 90 percent of the sites collected personal information from consumers. However, for the privacy criteria generally perceived as embodying fair information practices, such as consumer notice, consumer choice, access, security and contract information, the raw numbers from the survey are sobering. Only 9.5 percent of the entire survey sample contained these basic privacy criteria. Even at the top 100 most visited websites, only 19 percent have privacy policies consisting of accepting fair information practice criteria.

It is one thing to post your privacy policy, but it is an entirely separate issue as to whether or not that posted policy is anything more than a grudging acknowledgment that a website collects and discloses personal information without any consumer control over such collection of disclosure.

I hope we can make progress on that issue, as well as making progress on the encryption policy. It is the flip side of the same coin, and I believe that the industry has the same obligation to consumers in protecting them against companies compromising personal information as they do protecting them from the government compromising their personal information. From the consumer's perspective, there is no difference; and I am going to ask the witnesses today to tell me how they stand on this issue.

I thank you, Mr. Chairman.

Mr. TAUZIN. Thank you, Mr. Chairman, Mr. Markey.

We are pleased now to welcome the chairman of the full committee, the gentleman from Richmond, Virginia, Mr. Bliley. Since he is the most important member here, we will encrypt his testimony. We will supply you with it encoded.

Mr. Bliley, for an opening.

Chairman BLILEY. Thank you, Mr. Chairman. I want to thank you for yielding to me and holding this hearing.

The subcommittee meets to consider H.R. 850, a bill to provide export relief for certain encryption production. This is not a new issue. The Commerce Committee reported export relief legislation 2 years ago.

In 1997, we learned firsthand how contentious and important this issue is to all parties involved. The law enforcement and intelligence communities argued passionately that the current policy is workable and necessary for them to do what we expect from them. On the other hand, the high-tech community, the companies that are fueling our Nation's economies and producing dramatic innovation, argues strongly that the current policy is based on faulty logic and is directly harmful to their ability to compete internationally. They also point out that, while they are harmed by U.S. policy, American consumers and the growth of electronic commerce are harmed just as well.

The Commerce Committee has been a leader in opening the landscape for electronic commerce. We take seriously our role in promoting electronic commerce; and, for instance, I have introduced legislation dealing with the electronic signatures and the scope of data base protection, both of which the committee will turn to very soon. I support the effort to revise our Nation's export policy with regards to encryption to reflect a current availability of encryption products and the benefits of stronger products.

The administration's policy of today is unworkable and an impediment to the U.S. encryption producers and users. We need the policy to change. It is hard to restrict U.S. companies from selling 128-bit encryption products when the same product can be bought from an Israeli, French or Irish company. The administration has tried to minimize opposition to its policy by providing limited relief for certain sectors in certain type of companies.

This policy is partly based on the idea that containing U.S. encryption products will aid our national security. The administra-

tion has attempted to sell this approach in an international forum with little success or resulting in vague promises.

The current piecemeal encryption policy does nothing for the multiple companies that want to integrate encryption into their products as an add-on future. For instance, foreign software companies selling word processing products are using the U.S. restrictions as a marketing tool to sell their products over American companies. This current policy also lets uncertainty rule the day. We have been in contact with numerous electronic commerce firms that are trying to fight through the new rules to figure if they qualify or don't qualify for licensing exception and thus are able to provide service consumers want.

With that said, I am always interested in trying to find a compromise, if possible. If there is room for agreement that can help law enforcement or protect national security without codifying the current policy, I want to know about it.

We will move encryption legislation soon in this committee, and is H.R. 850 the best approach to do this? Should changes be made to the bill? Should we consider another approach like the one introduced by Senator McCain in the Senate?

I look forward to hearing from the panelists today on these important issues; and thank you again, Mr. Chairman, for yielding me the time.

Mr. TAUZIN. I thank you, Mr. Chairman, the leader of the Virginia high-tech crowd. I read about you guys in The Washington Post.

I am pleased now——

Chairman BLILEY. Don't believe everything you read in the Post.

Mr. TAUZIN. The Chair is pleased now to welcome the ranking minority member of the full committee, the Honorable John Dingell from Michigan.

Mr. DINGELL. Mr. Chairman, thank you for the recognition; and, Mr. Chairman, thank you for holding this hearing today. It is very important. This is not an easy subject. The committee has grappled with this matter for a number of years. Unfortunately, we have had little success in finding the right solution.

As each day goes by, technological advances create a greater need for a coherent national policy. I hope that, as the need for that solution becomes more compelling, this committee will redouble its efforts to find a sensible, rational middle ground that balances the crucial interests at stake.

We lead the world in production of computer hardware and software. Technology is an engine which drives the global economy and drives the U.S. economy. We should not idly sit by and let U.S. companies lose in the marketplace because they cannot deliver the kind of secure products and services customers demand.

But as we will hear from our witnesses today, I am sure, the advent of increasingly sophisticated technologies is a double-edged sword. It can make global commerce and communications more secure. It can also make national security and law enforcement less so. We all know too well even in the post-Cold-War era the wars against international terrorism, espionage and human rights abuses continue unabated, and significant threats exist to this country from activities of people, not its friends, both in the mili-

tary and espionage sense, and also from the standpoint of crime, drugs and matters of that sort.

Mr. Chairman, we have an important duty to see to it that we protect all of the vital interests of the United States in foreign commerce and communications. Thus, we have an important need to address the concerns of the administration with regard to security, which is very difficult. I am not quite sure how it can done or how it will be done, but I hope that we will work very hard on this particular point. And I am prepared to work with you to try and craft a sensible, national encryption policy we can all support.

I yield back the balance of my time.

Mr. TAUZIN. I thank the gentleman from Michigan.

And the Chair is now pleased to recognize the vice chairman of the subcommittee, the gentleman from Ohio, Mr. Oxley.

Mr. OXLEY. Thank you, Mr. Chairman, and welcome to our distinguished witnesses.

Mr. Chairman, I take a back seat to no one when it comes to matters of international free trade, U.S. export promotion, and support for our high-tech industries. You will find not a stronger advocate for U.S. firms seeking to penetrate foreign markets.

American companies are world leaders in encryption and other cutting edge technologies. They should be able to export their products to our trade partners around the globe. In fact, I would support the legislation before us if it were needed and took into serious account U.S. national security interests.

There is no doubt in my mind that American firms have the ability to produce the most powerful, most impenetrable encryption products in the world.

I do not question the value of this technology for purposes of protecting electronic commerce, consumer privacy, and proprietary information. We need this technology, and so do our trading partners.

We do not, however, need this legislation. It is unnecessary, given the administration's regular review and modernization of U.S. encryption policy. More importantly, the bill as drafted, it represents a real theft to national security and public safety in the United States.

I would refer the members to the closed briefing that we received last year from the various security agencies, including the FBI and the CIA. I would certainly recommend that we have a similar briefing before we move on this bill.

Mr. Chairman, there can be no doubt that the power of encryption technology in criminal hands or the hands of enemies of the United States can be turned to ill purposes with devastating consequences for members of a free society. I am speaking here of terrorists, antigovernment militants, rogue regimes, organized crime syndicates, drug cartels, child pornographers, kidnapers, pedophiles.

Not only would this legislation assist those who would use this technology to conceal their crimes from surveillance by our intelligence and law enforcement agencies, it would also undercut international efforts to control the proliferation of unbreakable encryption.

The enactment of H.R. 850 would make powerful encryption all the more available to our adversaries. It would undermine the

agreement reached last December to improve multilateral export controls under the Wassenaar Agreement. The 33 signatories to that agreement represent the bulk of encryption-producing countries.

Furthermore, this legislation is not necessary. The administration has provided significant relief from the export controls where it can safely do so, which I applaud.

Fifty-six-bit encryption products may be exported after a one-time review. Products above 56 bits may be exported for use by the subsidiaries of American firms, except those located in terrorist nations. They may be exported to 45 friendly nations to be used by banking, financial, medical, insurance, and on-line companies. Products above 56 bits may also be exported to other commercial firms if they are recoverable, as in the industry-developed "doorbell" approach.

Mr. Chairman, this is the kind of careful, reasoned approach to relaxing our export controls that is called for in a matter of this seriousness. I find it highly ironic that on the day that we receive the recommendations of the bipartisan commission report on high-tech transfers to China, which includes suggestions to strengthen our export system, we are considering legislation to undermine our multilateral export control system for encryption. It is unwise, and I fear we will live to regret it.

I yield back the balance of my time.

Mr. TAUZIN. Thank the gentleman.

The Chair is now pleased to recognize the gentleman also from Ohio, Mr. Sawyer, for an opening statement.

Mr. SAWYER. Thank you, Mr. Chairman, for the recognition and for having this hearing.

It has been almost 2 years since the subcommittee held its last hearing on this subject. The full committee passed it at the end of September in 1997. This bill never came to the floor, as you well know.

Not much has changed since that time in terms of the United States' policy and allowing companies to manufacture, use, and sell stronger encryption products. We continue to limit the availability of strong encryption, while discouraging exportation of encryption software.

What really has changed is we have a new chairman of the Rules Committee. I am not sure what his positions on this kind of legislation are, but it may make a difference.

I hope the subcommittee and the full committee will once again have the resolve to address the issues that are raised by H.R. 850.

Let me just say that I recognize the concerns of the law enforcement community. I think we need, as several members have mentioned, to find ways to address those concerns and make sure they have the tools to do their jobs effectively. But it just seems to me that for some time the genie has been out of the bottle. In fact, we have a bottle whose neck is very tightly sealed, the cork is embedded and very much in place, but there is no bottom left on the bottle. And that is a reality that we simply have to be able to address.

We are in a new era, as everybody is fond of saying. We have simply got to alter our policy to give consumers greater insurance that their communications and data are as private as possible and

so that we might compete with our international counterparts, particularly American companies that find themselves doing business throughout the world, in settings where they need to be as protected as they like to feel at home.

Mr. Chairman, let me thank you again for scheduling this hearing. I look forward to hearing from our witnesses.

Mr. TAUZIN. I thank my friend; and the Chair now yields for an opening statement to the gentleman from Illinois, Mr. Shimkus.

Mr. SHIMKUS. Thank you, Mr. Chairman.

I just want to welcome the panel, and I will turn back my balance of time to get started.

Mr. TAUZIN. The Chair will recognize the gentleman from Maryland, Mr. Ehrlich, for an opening statement.

Mr. EHRLICH. I have no opening statement. I would like to make a brief comment.

As a new member of the committee, this is certainly one of the more difficult issues that has been brought to my attention. I look forward to the comments of the panel, the impressive panel before us. What makes it very difficult, people for whom I have great respect in this area have quite diverse views, to say the least. So I look forward to a very good debate today.

Thank you, I yield back.

Mr. TAUZIN. I thank the gentleman.

I might point out the Chair has presented to me a letter from the Louisiana Sheriff's Association in favor of H.R. 850, I don't know how it is in Maryland. The Sheriffs have a good voice in Louisiana.

The gentleman from Georgia, Mr. Deal.

Mr. DEAL. Mr. Chairman, I don't have an opening statement.

Mr. TAUZIN. The gentleman from Oklahoma, Mr. Largent.

Mr. LARGENT. No.

[Additional statements submitted for the record follow:]

PREPARED STATEMENT OF HON. CLIFF STEARNS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA

Mr. Chairman: Thank you for calling this hearing on the important issue of encryption and the legislation before sponsored by our colleague, Mr. Goodlatte.

After being briefed by FBI Director Freeh during the last Congress before the mark-up of the same legislation, I was quite concerned with the security implications of allowing unimpeded export of encryption.

With the current atmosphere of widespread espionage being committed by the Communist government of China, I am even more concerned with the export of such encryption products. just imagine the Chinese encrypting the nuclear secrets, missile technology, or computer codes they have stolen from us.

I want to be assured that the passage of this legislation will not lead to dangerous China becoming more dangerous with the ability to import U.S. encryption products.

Of course under this Administration, the Chinese have probably already stolen whatever encryption material they could.

I voted in support of the Goodlatte bill last Congress in Committee, but supported the effort of Mr. Oxley in his amendment to restrict exportation for reasons of security and law enforcement. I look forward to the testimony of the witnesses in regard to efforts to amend this legislation to further protect U.S. national security.

I also look forward to the witness testimony regarding the compromise plan that was put forward into use by the Department of Commerce and whether new legislation is truly needed.

Finally, I would like the witnesses to address the economic impacts that restriction of encryption products has on U.S. businesses and whether current U.S. policy is simply forcing U.S. encryption producers to move off shore and sell their products unimpeded.

Thank you Mr. Chairman.

PREPARED STATEMENT OF HON. BARBARA CUBIN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF WYOMING

Thank you, Mr. Chairman, for holding this important hearing on H.R. 850, the Security And Freedom through Encryption (SAFE) Act.

I was a cosponsor of H.R. 695, originally introduced by Rep. Bob Goodlatte (R-VA) in the last Congress. Unfortunately that bill wasn't passed into law.

However, I have once again joined Congressman Goodlatte in supporting legislation, this year in the form of H.R. 850, to ensure the confidentiality of electronic messages and provide for a realistic and clear national encryption policy.

Among other things, H.R. 850 would somewhat ease U.S. export controls on encryption products, thereby providing U.S. individuals and companies with a greater ability to compete in the international marketplace.

This Administration has an unfortunate reputation for not providing a level playing field for American businesses to compete with overseas competitors in a global market.

I will be interested to hear from the witnesses today to learn what the Administration is doing to provide and maintain a business climate that encourages the development of information technology and encryption software and hardware.

If we expect e-commerce and other electronic transfers to continue to grow by leaps and bounds we must ensure that those transfers are safe and secure.

Currently, there are no federal restrictions on domestic encryption use, and H.R. 850 would not change this situation. However, last year there was a move in the full Commerce Committee to amend the bill to place certain restrictions on domestic encryption use.

Instead of adopting domestic restrictions, I'm pleased that the Commerce Committee approved a substitute amendment which would have, in part, reaffirmed the policy of no domestic restrictions and would have required the Commerce Department to conduct an expedited study of the issue of mandating a system for encryption recovery.

Encryption policy is a difficult balancing act. It forces us to walk a razor thin line between guaranteeing national security and protecting people's privacy.

I believe H.R. 850 is an appropriate and realistic approach to solving this vital national encryption issue.

Mr. Chairman, it is my hope that the Committee moves quickly to pass this important piece of legislation. I yield back the balance of my time.

PREPARED STATEMENT OF HON. ANNA ESHOO, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Thank you, Chairman Tauzin, for calling this hearing on H.R. 850, the SAFE Act.

I'm pleased that my constituent Tom Arnold representing CyberSource, is testifying before our Committee today. After working for NASA at the Ames Research Center in Mountain View, Mr. Arnold went to the private sector. We look forward to your testimony.

The SAFE Act currently has 252 cosponsors, far more than a majority of the Members of this House. A majority of the members of this Committee are cosponsoring this bill. And this Legislation is virtually the same bill that passed the full Commerce Committee last Congress.

Most if not all of us on the Commerce Committee have heard the arguments for and against this legislation.

What some may not realize is the development of a cottage industry, directly linked to the Administration's export control policy. We will hear today about foreign companies like Siemens, Phillips, and Entrust who face little or no restrictions on exporting encryption products.

CYBERNETICA, an Estonian data security company, is marketing its encryption product as having "No Export Restrictions."

These companies are flourishing due to our Administration's encryption policy. More importantly, U.S. companies are suffering.

Consumer demands and technological innovations have driven the development of encryption technology globally. Commerce Secretary Daley reported that consumers spent more than $9 billion online last year. Further, Forrester Research has predicted that E-commerce sales will reach $108 billion by 2003.

Recent studies also show that the Administration's encryption policy threatens to cost our economy from $60 to $90 billion dollars and 200,000 jobs over the next few years.

This legislation ensures that U.S. jobs are not lost to foreign companies due to our outdated export control policy.

In a global economy that is increasingly not restricted by boundaries, we no longer can maintain an export control policy restricted solely to within our borders.

Strong encryption is a key building block of the emerging information based economy. It is essential to high growth areas of the New Economy such as E-commerce, online banking, and maintaining the security of critical information.

Just over two weeks ago, the Ninth Circuit Appeals Court affirmed an earlier decision that in the name of national defense, the U.S. government should not restrict the very liberties it is supposed to be defending, exemplifying the judicial branch's understanding of the encryption debate.

It is now time for the Legislative Branch to follow suit and pass the SAFE Act.

I look forward to working with you Mr. Chairman on passing this bill through our Committee expeditiously.

Mr. TAUZIN. Then the Chair is very pleased to welcome our panel now.

I understand some of you, Ms. McNamara and Mr. Reinsch, have time delays, so we will try and go through this quickly. Let me urge you, with a large panel, we have your written statements in front of us, which we can read and review. If you would use your 5 minutes wisely, by summarizing, by conversationally giving us your point of view and hitting the high points, what you want us to remember about your testimony today, we would appreciate it. That will give us time to engage you in a dialog as soon as we can and give you time to make your appointments this morning.

We will begin by introducing the Honorable Ronald D. Lee, Associate Deputy Attorney General, United States Department of Justice. And, Mr. Lee, we welcome your testimony, sir.

Mr. LEE. Thank you, Mr. Chairman. With the Chair's indulgence, I would ask that Mr. Reinsch precede me.

Mr. TAUZIN. If that is—I have no objection.

Mr. Reinsch, do you want to go first? You are on, sir.

Mr. REINSCH. We have a traveling show, Mr. Chairman; and we usually present it in the same order.

Mr. TAUZIN. This is William Reinsch, the Under Secretary of Commerce for Export Administration, the United States Department of Commerce.

Mr. Reinsch.

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

Mr. REINSCH. Thank you. I wouldn't want the subcommittee to think that we are incapable of innovation, but I think there is some flow to our comments that might make more sense if delivered in the right order.

Let me make an abbreviated version of my statement. I appreciate you putting the full one in the record.

It is a pleasure to be back, Mr. Chairman, to discuss one of my favorite subjects. We think we made some progress, notwithstanding the comments of some of the members of the committee, on our policy since the last time I appeared. It is obvious, though, even from this morning's remarks, that encryption remains a hotly debated issue.

We continue 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 marketplace.

The Internet and other digital media are becoming increasingly important to the conduct of international business. My full statement supplies a number of statistics on that point, and I won't go into that in detail.

It is clear, though, that in addition to the rapid growth of E-commerce, businesses also maintain their records and other proprietary information electronically. They conduct day-to-day communications and business transactions through the Internet and E-mail. An inevitable by-product of this growth is the need for strong encryption to provide the necessary secure infrastructure for digital communications, transactions and networks; and we support that. That is precisely why developing a new policy has been difficult—because we don't want to hinder the legitimate use of encryption, particularly for electronic commerce.

During the past 3 years, through extensive consultations with the Congress, people at this table and many others in the industry, we have concluded, among other things, there is no one-size-fits-all solution; and we have put out a variety of revisions to our policy to try to address the many different aspects of encryption.

Last September 22nd, we published a regulation implementing our decision to allow 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 economies.

A week earlier, on September 16th, the Vice President unveiled an overall update to our policy that addresses a number of the concerns that were expressed today by opening large markets and further streamlining exports.

That update permits the export of 128-bit encryption products and higher with or without key recovery to a number of industry sectors. Now banks, financial institutions, health facilities and online merchants can secure their sensitive financial, medical and online transactions in an electronic form. This update also allows U.S. companies to export 128-bit or greater encryption products, including technology to its subsidiaries located worldwide, to protect its proprietary information and to develop new products.

Many of the updates permit the export of encryption to these end users under a license exception. That is, after a technical review it could be exported by manufacturers, resellers and distributors without the need for a license or other additional review.

Our policy is to approve exports of strong encryption to a list of countries or a set of end users, rather than permit exports globally, to help protect national security interests. However, we do have a general policy of approval through encryption licensing arrangements, similar to bulk licenses, which allow unlimited shipments of strong encryption to these sectors worldwide.

Furthermore, our update allows the export of 128-bit or greater recovery capable or recoverable encryption products under

encryption licensing arrangements. 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.

There has been some talk in the opening statements about our international efforts. In December, through the hard work of Ambassador Aaron, the President's special envoy, the Wassenaar Arrangement members agreed on several changes relating to encryption controls.

Specific changes to multilateral encryption controls include removing multilateral controls on all encryption products at or below 56 bits and certain consumer items regardless of key length.

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

Let me be clear, Mr. Chairman, this does not mean that encryption products of more than 64 bits cannot be exported. As I just said, our own policy permits that, as do the policies of most other Wassenaar members. It does mean there has to be a national review.

Mr. Chairman, let me just say, with respect to H.R. 850, briefly, it will come as no surprise to you that the administration opposes this bill, as we did before; and my full statement goes into greater detail on that.

Let me just say that we believe the bill in letter and spirit will destroy the balance we worked so hard to achieve. It would jeopardize our law enforcement and national security interests; and we believe that the best way to make progress on this issue is through further constructive dialog with the Congress, with the industry, and with its many customers.

Thank you very much.

[The prepared statement of William A. Reinsch follows:]

PREPARED STATEMENT OF WILLIAM A. REINSCH, UNDER SECRETARY FOR EXPORT ADMINISTRATION, 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.

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. One of the many uses of the Internet which will have a significant effect on our everyday lives is electronic commerce. 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 electronically. 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 a new 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 plaintext 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 in lawful access. There is no one-size-fits-all solution. The plans for recovery encryption products we received from more than sixty 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 learned that the use of strong non-recovery encryption within certain trusted industry sectors is an important component of our policy in order to protect private consumer information and allow our US high tech industry to maintain its lead in the information security market while minimizing risk to national security and law enforcement equities. Taking into account all that we have learned and reviewing international market trends and realities, in 1998 we made several changes to our encryption policy that I will summarize for you.

On September 22, 1998, we published a regulation implementing our decision to allow the export, under a license exception, of unlimited strength encryption to banks and financial institutions located in countries that are members of the Financial Action Task Force or which have effective anti-money laundering laws. This regulation also allows exports, under a license exception, of encryption products that are specially designed for financial transactions. This policy recognizes the need to secure and safeguard our financial networks, and that the banking and financial communities have a history of cooperation with government authorities when information is required to combat financial and other crimes.

As I mentioned earlier, we have been looking for ways to make our policy consistent with both market realities and national security and law enforcement concerns. For more than a year, the Administration has been engaged in 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 important privacy concerns. The purpose of this dialogue was to find cooperative solutions that could assist law enforcement while protecting national security, plus assuring continued U.S. technology leadership and promoting the privacy and security of U.S. firms and citizens in electronic commerce. We believed then and now that the best way to make progress on this issue is through a constructive, cooperative dialogue, rather than seeking legislative solutions. Through our dialogue, there has been increased understanding among the parties, and we have made progress.

The result of this dialogue was an update to our encryption policy which Vice President Gore unveiled last September 16. The regulations implementing the update were published on December 31. This 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 reduced controls on exports of 56-bit products and, for certain industry sectors, on exports of products of unlimited bit length, whether or not they contain recovery features. In developing our policy we identified key sectors that can form the basis of a secure infrastructure for communicating and storing information: banks, a broad range of financial institutions, insurance companies, on-line merchants, and health facilities. 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. Specifically, the new policy allows for:

- exports of 56-bit software and most hardware to any end user under a license exception;
- exports of strong encryption, including technology, to U.S. companies and their subsidiaries under a license exception to protect important business proprietary information;
- exports of strong encryption to the insurance and medical/health sectors in 46 countries under a license exception for use in securing proprietary medical and health information;
- exports of strong encryption to secure on-line transactions between on-line merchants and their customers in 46 countries under a license exception.
- "recovery capable" or "recoverable" encryption products of any key length, such as the "Doorbell" products developed by a number of companies, can now be approved under a kind of bulk license called an "encryption licensing arrangement" to recipients in located in 46 countries. Such products include systems that are managed by a network or corporate security administrator.

I would note that these provisions apply to exports of products with or without key recovery features. One of the aspects of our policy update is to permit exports of strong encryption with or without key recovery to protect electronic commerce while also minimizing the risk to national security and law enforcement. For example, in some cases we have limited our approval policy to a list of countries or a set of end users, rather than permit exports on a global basis, to help protect national security interests.

We have also expanded our policy to encourage the marketing of a wider variety of "recoverable" products that may not be key recovery in a narrow sense but which may be helpful to law enforcement acting pursuant to strict legal authorities. Again, these are typically systems managed by a network or corporate administrator. 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.

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 civilian items 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 permit the export of mass market encryption software without restriction. The GSN was created to release general purpose software used on personal computers, but it inadvertently encouraged some signatory countries to permit the unrestricted export of encryption software. 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 result in government review of the dissemination of mass market software of up to 64 bits.

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 must be reviewed by governments consistent with their national export control procedures.

Export control policies without a multilateral approach have little chance of success. Agreement, by the Wassenaar members, to close the loophole for mass market encryption products is a strong indication that other countries are beginning to 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 harmonized international approach to encryption controls.

At the same time, we recognize that this is an evolutionary process, and we intend to continue our dialogue with industry. Our policy should 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.

With respect to H.R.850, the Administration opposes this legislation as we did its predecessor in the last Congress. The bill proposes export liberalization far beyond what the Administration can entertain and which would be contrary to our international export control obligations. Despite some cosmetic changes the authors have made, the bill in letter and spirit would destroy the balance we have worked so hard to achieve and would jeopardize our law enforcement and national security interests. I defer to other witnesses to describe the impact of the bill on their equities, but let me describe two of its other problems

First, I want to reiterate that this Administration does not seek controls or restraints on domestic manufacture or use of encryption. We continue to believe the best way to make progress on ways to assist law enforcement is through a constructive dialogue. As a result, we see no need for the statutory prohibitions contained in the bill. Second, once again we must take exception to the bill's export control provisions. In particular, the references to IEEPA as I understand them might have the effect of precluding controls under current circumstances and in any future situation where the EAA had expired, and the definition of general availability, as in the past, would preclude export controls over most software.

In addition, whether intended or not, we believe the bill as drafted could inhibit the development of key recovery even as a viable commercial option for those corporations and end users that want it in order to guarantee access to their data. The Administration has repeatedly stated that it does not support mandatory key recovery, but we endorse and encourage development of voluntary key recovery systems, and, based on industry input, we see growing demand for them, especially corporate key recovery, that we do not want to cut off.

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 so that it can continue to promote our economic, foreign policy and national security interests while adjusting 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 this Committee knows better than most, public debate over encryption policy has been spirited. Many in the debate have had difficulty grasping different views or realizing that there is a middle ground. 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 US companies.

Mr. TAUZIN. Thank you.

Mr. Reinsch, the reason—I will hear from all the witnesses, but if you have to leave before we get to it, one of the things that I want you to respond in writing to is, what will be the administration's position if the Ninth Circuit decision is upheld on that appeal, and how do you plan to respond to it? It is going to be a serious question.

Mr. REINSCH. I can do that right now, Mr. Chairman.

Mr. TAUZIN. I don't want to interrupt. I want to get everybody in.

And the other thing we may want more information on is more detail on why you think the draft of H.R. 850 inhibits the development of voluntary key recovery systems. We would like to understand that argument a little better.

Mr. TAUZIN. The Chair will now turn back to Mr. Lee for his testimony.

STATEMENT OF HON. RONALD D. LEE, ASSOCIATE DEPUTY ATTORNEY GENERAL, DEPARTMENT OF JUSTICE

Mr. LEE. Thank you, Mr. Chairman. I have prepared a written statement, and I will just try to summarize it here.

The Department of Justice and law enforcement agree with the comments of several members and the Chair that strong encryption is coming. It is needed. It is needed to protect the privacy of American citizens. It is needed to promote the security of, and the confidence that the public places in, our information infrastructure.

We would be remiss, however, if we did not also state our deep concern about the threat to public safety posed by the widespread use of encryption in the hands of criminals and terrorists. Law enforcement agencies, Federal, State and local here in the United States, and their counterparts in foreign countries, have already begun to encounter the use of encryption in attempts to conceal criminal activity.

We believe that with the growth of encryption and the growth of digital media generally, the number and complexity of these cases will certainly increase as encryption becomes increasingly a feature of our lives.

We must recognize the very real costs to public safety that the use of encryption by criminals poses. The net result is easy to state. Agents frequently will not be able to make effective use of search warrants, wiretap orders and other legal processes, authorized by Congress and ordered by the courts after searching review, that are essential to effective law enforcement investigations today. It will be harder and harder to investigate, to find evidence of criminal activity and to prosecute that activity.

In the light of these challenges, the Department of Justice supports the carefully balanced approach to export controls that Secretary Reinsch laid out.

The Attorney General, along with the Director of the Federal Bureau of Investigation and other government officials, has been engaging industry leaders in a continuing and cooperative dialog. This dialog has gone on at several levels; and it has provided us both with an opportunity to explain our public safety concerns and, just as importantly, perhaps more importantly for our learning curve, to learn about innovative solutions that industry has presented.

Both we and industry have found the discussions to be candid and productive. We are committed to continuing those discussions. We believe that the current balanced approach is most conducive to continuing this dialog and these lines of communication.

The rapid elimination of export controls as proposed in the Security and Freedom Through Encryption Act would upset this bal-

ance. We believe that passage of the SAFE Act would cause the further spread of robust encryption products that would be used by terrorist organizations and other criminals to conceal their activities and would frustrate the ability of law enforcement to conduct effective investigations.

We realize that law enforcement has an obligation to develop its own resources to deal with this problem, as well as reaching out to others. We have begun initiatives such as the funding of a centralized technical resource within the FBI which will support Federal, State and local law enforcement personnel to develop a broad range of expertise, technologies and tools. These items will help us respond directly to the threat of public safety that the use of strong encryption poses. This resource will also help law enforcement stay abreast of current technology.

We look forward with working with Congress, with Congressman Markey and others in discussing this topic so that law enforcement may continue its mission of protecting public safety into the future. We do have to explain, however, that no matter what technology, no matter what resources are developed, there is no silver bullet, there is no one solution that the administration and Congress can point to and say, this offers law enforcement what it needs. Widespread use of nonrecoverable encryption will quickly overwhelm any possible silver bullet that could be developed now or in the future.

In light of that, we need to rely on the balanced approach that we are pursuing. This approach balances the need for secure, private communications with the equally important need to protect the safety of the public against threats from terrorists and criminals. We believe that our counterparts in foreign law enforcement share these concerns. We look forward to working with you on this important issue now and in the future.

Thank you, Mr. Chairman.

[The prepared statement of Ronald D. Lee follows:]

PREPARED STATEMENT OF RONALD D. LEE, ASSOCIATE DEPUTY ATTORNEY GENERAL, DEPARTMENT OF JUSTICE

Mr. Chairman, thank you for the opportunity to testify about the Department of Justice's views on export controls on encryption, and particularly the proposed Security and Freedom through Encryption (SAFE) Act, introduced by Mr. Goodlatte as H.R. 850. As you are aware, export controls on encryption is a complex and difficult issue 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 SAFE Act.

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, hacking or theft of confidential information. Over the last few years, the Department has continually pressed for the protection of 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.

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, even while we favor the spread of strong encryption products that permit timely and legal law enforcement access to the plaintext of encrypted, criminally-related information.

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 dependent on 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 still not universal, we have already begun to encounter its harmful effects. For example, in an investigation of a multi-national child pornography ring, investigators discovered sophisticated encryption used to protect thousands of images of child pornography that were exchanged among members. Similarly, in several major 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. 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.

Export controls on encryption products have been in place for years and exist primarily to protect national security and foreign policy interests. The nation's intelligence gathering efforts often provide valuable information to law enforcement agencies relating to criminal or terrorist acts, and we believe that this capability cannot be lost. Nonetheless, U.S. law enforcement has much greater concerns about the use of non-recoverable encryption products by criminal elements within the United States that prevent timely law enforcement access to the plaintext of lawfully-seized encrypted data and communications relating to criminal or terrorist activity.

The Department of Justice, and the law enforcement community as a whole, supports the use of encryption technology to protect data and communications from unlawful and unauthorized access, disclosure, and alteration. Additionally, encryption helps to prevent crime by protecting a range of valuable information over increasingly widespread and interconnected computer and information networks. At the same time, we believe that the widespread use of unbreakable encryption by criminal elements presents a tremendous threat to both public safety and national security. Accordingly, the law enforcement community supports the development and widespread use of strong, recoverable encryption products and services.

The Department believes that encouraging the use of recoverable encryption products is an important part of protecting business and personal data as well as protecting public safety. In addition, this approach continues to find support among businesses and individuals that foresee a need to recover information that has been encrypted. 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. 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 data recovery products, rec-

ognizing that only their ubiquitous use will provide both protection for data and protection of public safety.

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, consumers, 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.

We believe that a constructive dialogue on these issues is the best way to make progress, rather than seeking export control legislation. Largely as a result of the dialogue the Administration has had with industry, significant progress was 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 liberalized controls on products that have a bit length of 56-bits or less, and permit the 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 personal information, to use products that will protect the privacy of their clients. We also expanded our policy to permit recoverable exports, such as systems managed by network administrators, to foreign commercial firms. We learned about these systems through our dialogue with industry, and they are largely consistent with the needs of law enforcement. In addition, 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.

At the same time, 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.

The proposed Security and Freedom through Encryption Act raises several concerns from the perspective of the Department of Justice. First, we share the deep concern of the National Security Agency that the proposed SAFE Act would harm national security and public safety interests through the liberalization of export controls far beyond our current policy, and contrary to our international export control obligations. We are similarly concerned that a decontrol of unbreakable encryption will cause the further spread of robust encryption products to terrorist organizations and international criminals and frustrate the ability of law enforcement to combat these problems internationally.

The second problem is that the Act may impede the development of products that could assist law enforcement to access plaintext even when also demanded by the marketplace. The Administration believes that the development of such products is important for a safe society. Unfortunately, to the extent that this provision would actually prohibit government from encouraging development of key management infrastructures and other similar technologies, the provision could preclude U.S. government agencies from complying with statutory requirements and would put public safety and national security at risk. For example, it might preclude the United States government from utilizing useful and appropriate incentives to use key recovery techniques. The government might not be able to require its own contractors to use key recovery or demand its use in the legally required storage of records regarding such matters as sales of controlled substances or firearms.

It is also important to consider that our allies concur that unrestricted export of encryption poses 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 national interests, including a strong U.S. industry and promoting electronic commerce, while simultaneously protecting law enforcement and national security interests. We believe that legislation that eliminates all export controls on encryption could upset that delicate balance and is contrary to our national interests.

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 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.

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 plaintext 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 Subcommittee as it enters the markup phase of this bill.

Mr. TAUZIN. Thank you, Mr. Lee.

I want to turn to Mr. Ed Gillespie, the Executive Director of Americans for Computer Privacy here in Washington, DC. Ed, for your testimony, sir.

STATEMENT OF ED GILLESPIE, EXECUTIVE DIRECTOR, AMERICANS FOR COMPUTER PRIVACY

Mr. GILLESPIE. Thank you, Mr. Chairman. Thank you for this opportunity to testify in support of H.R. 850, the SAFE act as sponsored by Representatives Goodlatte and Lofgren and cosponsored by a bipartisan support of over 250 Members of the House.

I serve as Executive Director for Americans for Computer Privacy, 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.

We applaud the chairman and ranking member of this subcommittee and majority of members of the Commerce Committee who have cosponsored the bill and respectfully urge the subcommittee to report it without amendments for full committee consideration.

ACP believes strong encryption is essential to protecting the Nation's infrastructure and ensuring the integrity——

Is that mine or his?

Mr. TAUZIN. It is a very sophisticated—the technologically sufficient system that we are working on.

Mr. GILLESPIE. We believe that strong encryption is essential to also ensuring the privacy of electronic communications of American citizens, businesses and organizations; protecting our long-term national security interests; safeguarding the public; and maintaining U.S. leadership in the development of information technology industries.

The United States must have a clear and realistic national policy to assure that industry is able to develop the products that will help us to meet our national objectives.

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.

Consumers worldwide demand to be able to protect their electronic information and interact securely, and access to products of strong encryption capability has been become critical to providing them with confidence that they will have this ability.

Progress was made last year in the development of the administration's policy as announced by the Vice President in September and contained in the interim final regulations. ACP commends the government for the hard work and thoughtful consideration that went into the development of that policy and those regulations.

However, the Clinton administration has yet to allow U.S. encryption manufacturers to compete on a level playing field in the global marketplace. The administration policy remains highly problematic and does not represent the clear and realistic national policy that this issue requires.

Primarily, ACP believes that the export policy shortchanges our long-term national interest and that it puts at jeopardy our current global leadership in this vital technology. Strong high-quality encryption products are already widely available from foreign makers that renders our export policy and exercise in futility. We worry that America will lose this critical market to foreign makers. When and if it does, it will be too late to change U.S. policy and too late to preserve our leadership in this vital arena.

There can be no doubt that U.S. national security objectives are best served by an information technology world in which U.S. companies are market leaders in all aspects, especially encryption. ACP's industrial members have ample evidence of the rapidly growing market share of foreign encryption and examples of U.S. businesses losing out to foreign manufacturers because of our U.S. export regulations.

A 1997 study found that 656 non-American encryption products are available from 29 foreign countries. These encryption manufacturers are located as far from the United States as India and as close to our borders as Mexico. The products in the study were purchased via routine channels or directly from the foreign manufacturer or from a distributor.

Strong encryption is also available for sale and for free on the Internet to anyone in the world with a computer. Here is just one example of how you can obtain strong encryption with just a few

clicks: You can visit the international Pretty Good Privacy Site: www.pgpx.com. From that URL, anybody in the world can develop strong 128-bit encryption within 47 seconds. And because any citizen in the U.S. can download encryption legally from the Internet, the Internet makes controlling encryption exports a very difficult proposition.

ACP strongly believes 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 math. That is what we are talking here. Encryption algorithms are nothing more than sophisticated mathematics. And while the U.S. may realistically hope to remain the leader in such a field, it cannot realistically expect to monopolize it.

ACP 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. However, Congress must pass the SAFE act and establish a clear and realistic national policy on encryption. That is the best way to preserve U.S. leadership encryption technology upon which the successful protection of our critical infrastructure and achievement of national security objectives certainly and inevitably depends.

Thank you again, Mr. Chairman; and I will look forward to your questions.

[The prepared statement of Ed Gillespie follows:]

PREPARED STATEMENT OF ED GILLESPIE, EXECUTIVE DIRECTOR, AMERICANS FOR COMPUTER PRIVACY

Mr. Chairman and members of the Subcommittee, Thank you for the opportunity to testify before you on H.R. 850, the SAFE Act, sponsored by Representatives Goodlatte and Lofgren and cosponsored by a bipartisan group of over 250 House Members. I serve as Executive Director of Americans for Computer Privacy ("ACP"), 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.

ACP strongly endorses enactment of the SAFE Act, and we appreciate the leadership provided by Representatives Goodlatte and Lofgren and the majority of members of the Commerce Committee who cosponsored the bill. We respectfully urge the subcommittee to report it without amendments for full committee consideration.

As Vice President Gore said in September 1998 when he announced the current administration policy, developing a national encryption policy is one of the most difficult issues facing the country. It requires balancing many competing objectives—all of which are of great importance to the nation. As ACP has noted, strong encryption is essential to:

- Protecting the nation's infrastructure and assuring the integrity of information;
- Ensuring the privacy of electronic communications of American citizens, businesses and organizations;
- Protecting our national security interests;
- Safeguarding the public; and
- Maintaining U.S. leadership in the development of information technology industry.

As we move into the new millenium, information technology will play an increasingly important role in the way we govern ourselves, communicate among peoples,

conduct commerce, and operate and protect our national infrastructure. Strong encryption is key to the continued vitality and growth of all these activities. Accordingly, the United States needs a clear and realistic national policy to assure that industry is able to develop the products that will help us to meet our national objectives.

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 and spending. More than 10 million people in North America alone have 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. 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.

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.

Significant progress was made last year in the development of the Administration's policy announced by the Vice President in September and contained in the interim final regulations of December 31, 1998. ACP commends the government for the hard work and thoughtful consideration that went into the development of that policy and those regulations. Last year, ACP had several productive meetings with the Administration's inter-agency task force, including representatives from law enforcement and the Justice Department. Those meetings were conducted in good-faith on both sides and led to a greater understanding on both sides of the needs and concerns of the other. The Clinton Administration incorporated many of our interim recommendations into its updated export policy, including: export relief for encryption products that use symmetric algorithms up to and including 56-bits; products that use asymmetric algorithms up to and including 1024-bits; and relief for various sectors of the business community.

The Clinton Administration, however, has yet to allow U.S. encryption manufacturers to compete on a level playing field in the global marketplace. The Administration policy remains highly problematic and does not represent the clear and realistic national policy that this issue requires.

First, the Administration has entered into an agreement with 32 other countries—the Wassenaar Arrangement—containing certain export controls on encryption. Unfortunately, the Administration's encryption export regulations impose greater restrictions on American companies than those called for under the arrangement. As a minimal interim step, we believe the Administration should at least eliminate all controls on encryption software and hardware for products up to 64-bits, and should eliminate all reporting requirements on higher- level encryption exports. Such actions would make U.S. controls consistent with the revised Wassenaar Arrangement.

We also believe that the Administration's efforts to develop a global approach to this issue through the Wassenaar Arrangement are doomed to failure. We recognize that this is a global problem and if it were truly possible to achieve universal agreement that was fairly enforced, industry would no doubt be supportive. But Wassenaar only has 33 members and does not include encryption-producing countries such as China, India, South Africa, or Israel. Further, the Administration should recognize that the Wassenaar Arrangement is only as effective as the implementing regulations adopted by the member countries. Some of the member nations will promulgate regulations that are less restrictive than those of the United States, thereby providing those nations with a competitive advantage over domestic encryption manufacturers. In short, the Wassenaar Arrangement is a toothless tiger.

As an example, I would point to a December 6, 1998 *New York Times* article that highlights the difficulty the Wassenaar Arrangement has encountered in attempting to restrict sales of combat aircraft and tanks to Ethiopia and Uganda; clearly, the problems associated with Wassenaar would be compounded when attempting to restrict products that fit on a compact disk or can be sent over the Internet.

Second, the Interim Rule falls short on a number of short-term points. For example, the Interim Rule does not fulfill the mandate promised by Vice President Gore on September 16 to allow all 56-bit encryption products to be eligible for export to all end-users (except terrorist states). In reality, the Interim Rule does not allow the

export of 56-bit encryption chips, integrated circuits, toolkits, and executable or linkable modules for export under license exception except to U.S. subsidiaries.

Further, the Interim Rule is so complex that a number of the benefits in the new policy are undermined by provisions of the Interim Rule. For example, the reporting requirements are so onerous to companies that reporting costs may exceed the price of some products, much less the profit. It is simply impractical to expect manufacturers to collect reporting data on mass-market encryption products. My personal experience is that I never return registration cards on coffee makers, answering machines, or software products—I expect most people in this room have similar experiences.

We have made these points in a letter providing our official comments on the regulations to the Administration. However, the Administration's new policy, as grateful as we are for this limited progress, remains flawed even on its own terms.

Beyond this, in the encryption debate in the larger sense, we continue to have good-faith disagreements with the Administration about its current policy, which Congress should address in this legislation.

Primarily, ACP believes that the export policy short-changes our long-term national interest in that it puts at jeopardy our current global leadership in this vital technology. Strong, high-quality encryption products already are widely available from foreign makers. That renders our export policy an exercise in futility. We worry that America will lose this critical market to foreign makers. When and if it does, it will be too late to change U.S. policy and too late to preserve U.S. leadership in this vital arena.

If we do lose that U.S. leadership position, what will that 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, if the most sophisticated encryption experts and product-makers reside abroad? It will also mean that the protection of our critical national infrastructure may depend on foreign-made encryption—and that's unacceptable.

We 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, there can be no doubt that 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. ACP's industrial members have ample evidence of the rapidly growing market share of foreign encryption and examples of U.S. businesses losing out to foreign manufacturers because of the U.S. export regulations. For example, a December 1997 study conducted by Trusted Information System found that 656 non-American encryption products are available from 29 foreign countries. These encryption manufacturers are located as far from the U.S. as China and as close as Mexico. The products in the study were purchased via routine channels, either directly from the foreign manufacturer or from a distributor.

RSA Data Security has lost business opportunities with major foreign conglomerates such as Lloyds TSB PLC, SAP AG, and Siemens Ag because of U.S. export control regulations. U.S. software companies estimate they have lost millions of potential users of their software due to the encryption regulations. ACP believes these foreign customers are purchasing strong, non-American encryption products. These foreign products are also of high quality and we do not accept the belief that these foreign entities are forgoing strong encryption just because they can't get American-made encryption.

Further, foreign encryption manufacturers are marketing their products by using U.S. encryption regulations against American companies. For example, Baltimore Technologies, an Irish encryption manufacturer that President Clinton highlighted during his trip to Dublin last year, specifically points out the shortcomings of U.S. encryption products in the marketing of their product, WebSecure. The opening paragraph of its website states that the export versions of U.S. browsers "are limited to 40 bits of encryption, which is not secure enough for most applications." In contrast, WebSecure provides 128-bit encryption for "real security." [1]

Strong encryption is also available for sale and for free on the Internet to anybody in the world with a computer. Here is just one example of the ease with which a person outside the United States can obtain strong encryption with a few clicks on their computer: They can visit the international Pretty Good Privacy site: www.pgpi.com. From that URL, anybody in the world can download strong, 128-bit encryption within 47 seconds. And because any citizen in the U.S. can download encryption legally from the Internet, and anyone in the world with a computer has

[1] Located at the following URL: www.baltimore.com/products/websecure/index.html

access to the Internet, the Internet makes controlling encryption exports a very difficult proposition.

ACP also believes it is vital to our national interests that our critical infrastructure is secure and we praise President Clinton for recognizing this vulnerability in his speech earlier this year. We wish, however, that the President recognized the importance that strong encryption produced by U.S. high technology companies plays in protecting our infrastructure. How does the United States protect its critical infrastructure? With strong encryption, that's how. And the current export controls are threatening the health of the very industry in which the protection of our critical infrastructure relies.

We do not believe we have all the answers to questions about national security, but ACP strongly believes 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."

For instance, ACP proposed last year the creation of a "NET Center" (and, since then, "Tech Center" has been created) to help law enforcement officials understand how to deal with encryption and other technological advances when encountered in a criminal setting. We have been cooperating with law enforcement agencies on these projects in an educational sense, and we are pleased with the development of this forward-thinking strategy.

On the national security side, Senator Bob Kerrey recently suggested that (1) the President should convene a public-private panel to examine the implications of this new technological age for our national security, and (2) the creation of a new national laboratory for information technology to perform research and to act as a forum for further discussions on technological breakthroughs. These views may deserve further exploration, and ACP wants to play a leading role in crafting industry cooperation.

ACP wishes to emphasize that it recognizes a legitimate governmental need to obtain access to the plain text of communications when authorized by proper legal authority. ACP and its members are responsible citizens of the nation and the globe and have no wish to facilitate the commission of crime, the spread of terrorism or the acquisition and delivery of weapons of mass destruction. Similarly, we are committed to strengthening the nation's infrastructure, enhancing the privacy of American citizens and ensuring the security of electronic commerce. We believe that these sometimes competing objectives can be met, but only if government does not seek to force solutions on the industry that are not compatible with the development of technology and market demands.

ACP 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.

I would also like to point out that earlier this month, the Ninth Circuit Court of Appeals upheld a district court ruling in *Bernstein* v. *U.S. Department of Justice* which found that the export controls at issue here are an unconstitutional prior restraint on speech. The Appeals Court affirmed the lower court's decision, and concluded that the Government's policy on encryption unconstitutionally burdens speech because it "applies directly to scientific expression, vests boundless discretion in government officials, and lacks adequate procedural safeguards."

The Ninth Circuit Court of Appeals also found, "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. Cel-

lular 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 neighbors, 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, see McIntyre v. Ohio Elections Comm'n, 115 S. Ct. 1511, 1524 (1995) , the right against compelled speech, see Wooley v. Maynard, 430 U.S. 705, 714 (1977), and the right to informational privacy, see Whalen v. Roe, 429 U.S. 589, 599-600 (1977)."

In closing, Secretary of Defense William Cohen gave a speech at Microsoft earlier this year in which he stated: "To maintain peace and stability in this uncertain world, we have mapped out a strategy defined by three words: Shape, Respond, Prepare." ACP and its member companies are willing to do our part in helping the Government prepare for an uncertain 21st century, and we look forward to working with the Government on these projects.

However Congress must pass the SAFE Act and establish a clear and realistic national policy on encryption. That is the best way to preserve U.S. leadership in encryption technology, upon which the successful protection of our critical infrastructure and achievement of our national security objectives certainly and inevitably depend.

Mr. TAUZIN. Thank you, Mr. Gillespie.

We are now pleased to recognize the Honorable Barbara McNamara, Deputy Director, National Security Agency. I want to tell how pleased we are that you grace this hearing. We thought NSA folks were all in dark suits and dark glasses, and you look great today. Thanks for being here.

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

Ms. MCNAMARA. Thank you very much, I am glad I can lighten your life. Thank you for the opportunity to appear before you today. And you do have my statement for the record.

Mr. TAUZIN. Yes, ma'am.

Ms. MCNAMARA. NSA plays a critical role in our national security. We as an agency have two missions. One is to ensure that the U.S. Government communications are secure and protected against prosecution by foreign hostile services. For that mission and that mission alone, we could support and do support a very strong U.S. industry in order to provide that service to the U.S. Government.

But we also have another mission, and that other mission is the one that I would like to speak to you today about. It is a mission to provide foreign intelligence to the U.S. Government and policy makers and military commanders. We have a responsibility and do intercept and analyze the communication 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, first and foremost, perishable. It is worthless if we cannot get it to the decisionmakers in time to make a difference.

Signals intelligence proved its worth in World War II. The United States broke the Japanese naval code and learned of their plans to invade Midway Island, significantly aided the U.S. defeat of the Japanese fleet and helped shorten the war.

Today, NSA provides exactly that same service to U.S. forces and coalition forces operating today in the Balkans. We have that responsibility to perform that support to our troops wherever it is that they operate in the world. Demands on NSA for timely intelligence support 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. And let me address, Congressman Sawyer's comments about the genie being out of the bottle. We acknowledge that there is strong encryption out there. In fact, my colleague here on my right addressed PGP. It is out there. But it is not being used broadly, and we know it is not being used broadly because that is our business. It is out there, it is not being used broadly and will not be used until a global security management infrastructure allows it to be used commonly across international borders.

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. decisionmakers. The SAFE Act mandates the immediate decontrol of most encryption exports which will greatly complicate our mission because it will take too long to decrypt a message if, indeed, we can decrypt it at all and respond to our global mission.

The bill would also prevent us from conducting a meaningful review of a proposed encryption export. These reviews provide us with valuable insight into what is being exported, to whom and for what purpose.

Congressman Oxley and Mr. Reinsch addressed the liberalization that occurred last year on the part of the administration, and Mr. Reinsch also addressed the international agreement.

Let me say in answer to your statement, Mr. Chairman, that what about—or your question—what about the other sectors that are not addressed in the liberalization that occurred last year? We do not automatically deny export of strong products to anyone. In fact, sectors of nations—we have approved export of very strong encryption products to areas of the world that are not part of the sectors that Mr. Reinsch described.

It is not automatic denial. We view them all in an individual licensed approach. So I would just like to put that statement on the record.

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

Let me close by taking advantage of Mr. Oxley's statement earlier. I would be more than pleased to talk in more detail in a classified hearing.

[The prepared statement of Hon. Barbara A. 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 SAFE Act. However, I would 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 grown 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 immediately 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 world'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 immediate 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. Immediate encryption decontrol will also deprive us of the

opportunity to conduct a meaningful review of encryption products prior to their export. In the past, this review process has provided 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, immediate 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 markets while trying to minimize potential risk to national security. We believe significant progress was made.

As you review the SAFE Act, it is very important that you understand the significant effect certain provisions of this bill will have on national security. If enacted, the bill would effectively decontrol most commercial computer software encryption and specified hardware encryption exports to all destinations, even regions of instability. It would also deprive the Government of the opportunity to conduct a meaningful review of a proposed export to assure it is compatible with U.S. national security interests and would also eliminate the ability to deny an export application if national security concerns are not adequately addressed.

The bill would permit exports of encryption based on products that are permitted to be exported for foreign financial institutions. The criteria for exporting encryption to these institutions should not be the basis for decontrolling other encryption exports. Allowing favorable treatment for specific classes of end-users may be appropriate in cases such as those involving banks and other financial institutions which are well regulated and have a good record of providing access to lawful requests for information. Requiring the blanket approval of exports to all other end-users in a country would eliminate important national security end-use considerations for these exports.

In summary, the SAFE 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 counter-terrorism 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 Subcommittee and I would be happy to answer any questions you may have.

Mr. TAUZIN. And we have noted Mr. Oxley's request, and we will probably give you that opportunity, Mrs. McNamara.

We are pleased now to welcome Mr. Richard Hornstein, the General Counsel of Network Associates, Inc. of Santa Clara, California.

Mr. Hornstein.

STATEMENT OF RICHARD HORNSTEIN, GENERAL COUNSEL, NETWORK ASSOCIATES, INC.

Mr. HORNSTEIN. Good morning.

My name is Richard Hornstein. I am the General Counsel of Network Associates. We are the world's leading provider of security products, software products. We are based in Santa Clara, California. Last year, Network Associates did approximately $1 billion of revenue. We have 2,700 employees worldwide, and we have offices located in 30 countries throughout the world.

I am also here to speak on behalf of the Business Software Alliance, the BSA. The BSA's members include, among others, Adobe, Lotus Development and Microsoft.

We would like to thank you, Mr. Chairman, as well as ranking member Mr. Markey, for your strong support in this and previous Congresses. We also want to thank the other 19 subcommittee members who are among the approximately 253 cosponsors of the SAFE act.

You may not know what Network Associates is. We were just recently born about a year ago through a merger of several companies, but probably you do know our products. Our products include Virus Scan, an antivirus product; Pretty Good Privacy, or PGP, an encryption, virtual private network; PKI products; Gauntlet firewall, that product is used by the NSA; Cybercop, which is an intrusion detection product.

These products we sell as individual point products, and we also sell them as an integrated suite. We look to providing to our customers solutions for their needs, and more and more our customers are demanding comprehensive solutions for their corporate needs.

If I can give you an example of how these products work. If you look upon a corporation as a village and if the village is going to need around it a castle wall to protect it, that will be a firewall. They would need soldiers to travel inside around the castle patrolling, checking I.D., making sure people aren't going where they are supposed to. That would be intrusion protection.

When the king needs to travel from his castle, travel across the countryside and go visit another castle, that will be either a virtual private network of communication or an encrypted E-mail message. I mean, this is in simplistic forms, really, what we are talking about here.

What I am looking at right now is, for us to grow as a company, we need to grow on a global basis. The time to market for our products is today. Our customers right now are looking for answers and solutions for us to provide today.

Foreign companies out there with comparable products are out there selling to our customers, the customers who buy Virus Scan

today. Checkpoint, an Israeli company, is selling firewall products on a worldwide basis. They have $150 million of revenue.

Baltimore Technologies, my counterpart is sitting down here, which is the UK Irish company, is selling virtual private networks and encryption products. They are a serious threat to our viability as an entity.

What I would like to do is give you a couple of examples of some deals that right now that we are looking at and questioning whether or not we actually will be able to get these deals.

One is with a company called DaimlerChrysler. It is a German company that is a major worldwide automaker. They also are a major U.S. company through their acquisition of Chrysler Motors. They are a customer of mine from the past because they lead license Virus Scan.

There is a seven-figure deal on the table today to license by a pretty good privacy PGP product. However, in competing on the bid on this product, on the sale of this product, I am up against a company called Eudomoako. Eudomoako is a German software security company. They did $35 million last year in revenue, and they are going rapidly right now all throughout Europe.

Right now, DaimlerChrysler, as I understand it in discussions with my sales folks, is stating that, yes, I can get your product, but I can't support—under the current rules, any sort of support that will be necessary for such a deal, hundreds of thousands of nodes today being sold to this customer, hundreds of thousands of nodes, would require technical support across the network. The only people appropriate to give such support are my engineers back in Santa Clara. They could not communicate with the German MIS departments without violating the technical assistance rules, exposing us to economic penalties and potential criminal sanctions.

A similar deal is for a company called Robert Bosch. This is an equipment company based out of Switzerland. Tens of thousands of nodes, six-figure deal, and I am in jeopardy of losing them to a company called Ascom, which is a billion dollar revenue Swiss hardware and software security company which is making inroads in the growing market.

Once these products are sold by our foreign competitors, it is like plumbing. You can't pull them out of the house. They are not going to replace me if in 2 or 3 years we liberalize these rules.

A third example is a company called Orient Overseas Container Line. This is a Pac Rim company. There, again, another company of mine that uses Virus Scan. This is, again, another six-figure deal.

I am up against in that transaction with Checkpoint, an Israeli company that sells a firewall—world-class firewall product and a VPN solution; and they are also bundling in the PKI Search Server, which is a Canadian product.

In speaking with my salesperson, as I understand it, Orient Overseas is not probably going to buy our product. Why? Because, in marketing, Checkpoint is looked to be the world leader. They are an Israeli company, and they are looked to be a dominant of 50 percent of the Pac Rim's market on firewalls and VPN products, virtual private networks.

Also, because of their VPN product or at least the network product has to be registered when such sales are made with the U.S. Government, the privacy concerns of my foreign customers are violated, and they don't want to buy my products because they don't to have a product that is being registered with any foreign government.

In closing, I would like to thank you for allowing me to speak here at this proceeding. I would like to thank you for—those of you for supporting the SAFE act. I can be available for any questions at your leisure.

Thank you very much.

[The prepared statement of Richard Hornstein follows:]

PREPARED STATEMENT OF RICHARD HORNSTEIN, VICE PRESIDENT OF LEGAL AFFAIRS, TAXATION AND CORPORATE DEVELOPMENT, NETWORK ASSOCIATES ON BEHALF OF THE BUSINESS SOFTWARE ALLIANCE

INTRODUCTION

Good Morning. My name is Richard Hornstein, and I am Vice President of Legal Affairs, Taxation and Corporate Development at Network Associates, Inc., at its headquarters in Santa Clara, California. Network Associates, Inc., is the leading independent worldwide supplier of enterprise-wide network security and management software. The array of security products offered by Network Associates includes: PGP e-mail and file (the leading e-mail encryption product providing secure encrypted communications for over six million users worldwide), the Gauntlet firewall (one of the leading commercial software firewall products originally developed for use by the NSA), PGP VPN (a revolutionary new Internet desktop communication product allowing users to communicate securely over the Internet distributing audio, video and text information on a secure encrypted channel across the Internet), and Cybercop (an intrusion software product which protects the computer network from internal/external intruders).

I greatly appreciate the opportunity to appear today before this Committee on behalf of Network Associates and the Business Software Alliance (BSA). 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, Intel, Intuit and Sybase. BSA websites: www.bsa.org; www.nopiracy.com.

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.

The Security and Freedom through Encryption (SAFE) Act, H.R. 850, modernizes U.S. export laws regarding software and hardware with encryption capabilities to permit American companies to compete on a level international playing field and to provide computer users with their choice of adequate protection for their confidential information and critical infrastructures.

For these reasons, BSA strongly supports the SAFE Act. We urge the Committee to report the SAFE Act unamended and look forward to its passage by the House this year.

We want to thank both you, Mr. Chairman, as well as Ranking Member Mr. Markey, for your strong support in this and previous Congresses. We also want to thank

the 19 other Subcommittee members who are among the 253 cosponsors of the SAFE Act.

This morning I want to make four points:

- The worldwide standard is 128-bit encryption;
- Mass market software and hardware is uncontrollable;
- U.S. manufacturers face unnecessarily a significant competitive disadvantage; and
- BSA strongly supports the SAFE Act because without relaxation of export controls, our critical infrastructures remain at risk. The inevitable result of the Administration's current policy will be widespread deployment, not of weak American software and hardware, but of foreign designed and manufactured strong encryption software and hardware throughout our infrastructures both in America and abroad.

WIDESPREAD DEPLOYMENT OF ENCRYPTION IS NOT ONLY DESIRABLE, IT IS CRITICAL

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 being choked by the lack of availability of strong encryption products.

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 and 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.

Full Deployment Of Strong Encryption Is Vital For Protecting 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.

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.

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. Thus, private businesses who are responsible for running our critical infrastructures and the millions of consumers transacting business over these infrastructures—depositing money in banks and purchasing airline tickets—must have access to the strongest security. This access cannot be limited to only American companies, however, as America's infrastructures cannot be protected if they are networked with foreign infrastructures limited to weak encryption.

In the long-term, we believe it is in America's best interest to have America's critical infrastructures and national security be protected by widespread reliance on strong *American* encryption products both here and abroad. The SAFE Act's encryption policy will ensure that Americans can use and sell any encryption that they want domestically, prohibit both Federal and State governments from imposing encryption standards or techniques, and relax export controls on products with encryption capabilities in a manner that is based on technological and market realities. Just because law enforcement and national security interests wish that they could turn back the clock and limit consumers' access to strong encryption approved by the government, it will not happen, especially on a worldwide basis. This is especially true for mass market software and hardware, which by its inherent nature is uncontrollable.

AMERICA'S EXPORT POLICY SHOULD PROMOTE WIDESPREAD DEPLOYMENT OF AMERICAN PRODUCTS WITH ENCRYPTION CAPABILITIES IN THE WORLDWIDE MARKET

Relaxation Of Export Controls On Encryption Products Is Vital For Ensuring America's Global Competitiveness

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 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. Between 1980 and 1992, the computing and software industry grew at an annual rate of over 28%, while overall domestic growth was less than 3%. 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.

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;
- The most widely used encryption program, PGP, with over six million users worldwide, uses the Swiss developed IDEA encryption algorithm, with a 128-bit key;
- 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 Con-

ference, 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, an Israeli computer scientist, 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 Crypytographic Research's latest meeting in Prague.

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.

Without Export Relief, Foreign Consumers Will Purchase Their Products From Foreign Suppliers, Keeping U.S. Manufacturers At A Competitive Disadvantage

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 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. An on-going industry study by Trusted Information Systems (TIS Study) highlights the ever-increasing availability of foreign developed and manufactured products as it discovered there were 656 foreign programs and products available from 29 countries as of December 1997.

Further demonstrating the worldwide availability, use and sophistication of encryption abroad is the Department of Commerce's National Institute of Standards and Technology (NIST) efforts to work with the private sector to develop an Advanced Encryption Standard (AES). Individuals and companies from eleven different countries proposed 10 out of the 15 candidate algorithms submitted to NIST: Australia's LOKI97; Belgium's RIJNDAEL; Canada's CAST-256 and DEAL; Costa Rica's FROG; France's DFC; Germany's MAGENTA; Japan's E2; Korea's CRYPTON; and the United Kingdom, Israel and Norway's SERPENT algorithms. Only 5 out of the 15 candidate algorithms were submitted by U.S.-based individuals or companies.

If an encryption product is combined with other applications such as Internet browsers and application servers, U.S. companies will generally 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.

I would like to mention a few specific examples with respect to foreign availability of encryption products. The Apache Group, based in the U.K., announced in April 1997 that its Apache Unix Internet Server software with very strong encryption had a 29% market share of Web server software. Today the Apache web server serves over half—50%—of the domains on the Internet.

Companies such as Brokat Informationssysteme, a German company, are developing products that are more than simply add-ons to American products. Brokat's modular e-services platform, Twister, which companies use to offer their customers secure and simple electronic services via various electronic channels, such as the Internet or mobile communications networks, is already being used by more than 1,500 companies worldwide. Brokat's sales outside of Germany, including to the United States, have now increased to be 56 percent of the company's total sales. The American market research institute Meridien Research described BROKAT as the leading company worldwide for Internet banking solutions. Apparently, in just a few years, we have already begun to loose our dominance of this critical infrastructure to a German company founded only in 1994.

The merger of two foreign companies, Zergo Holdings (U.K.) and Baltimore Technologies (Ireland), into a new company called Baltimore only further illustrates that foreign companies are flourishing solely because there is no U.S. competition. According to the Gartner Group in a Research Note dated January 28, 1999, the new company is "a competitive participant in providing e-commerce and enterprise security, with 11 international offices and a global partner network . . . with customers in 40 countries."

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.

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). We are only further accelerating the placement of foreign security products throughout the world in all industry infrastructures.

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 neighbors, 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 reso-

lution 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.

BSA STRONGLY SUPPORTS THE SAFE ACT BECAUSE IT PROVIDES FREEDOM FOR AMERICANS TO USE AND SELL ANY ENCRYPTION DOMESTICALLY AND PROVIDES GREATLY NEEDED EXPORT CONTROL RELIEF

The SAFE Act Preserves Americans' Domestic Encryption Freedom

The SAFE Act ensures that Americans may use and sell whatever kind of encryption they want domestically. It ensures that the U.S. government may not require or provide other incentives for Americans to use encryption products "approved" by the government or meeting certain standards. Also, the Act does not permit the government to link electronic signatures to the use of certain types of encryption products.

The SAFE Act Provides Law Enforcement With Important Safeguards

Importantly, the SAFE Act does permit the Secretary of Commerce to continue preventing exports to countries of terrorist concern or other embargoed countries pursuant to the Trading With The Enemy Act or the International Emergency Economic Powers Act. The bills also contain safeguards when relaxing export controls for strong encryption products—the Secretary of Commerce is not required to permit such exports if there is substantial evidence that the software or hardware will be diverted or modified for military or terrorist use or re-exported without requisite U.S. authorization.

The SAFE Act Recognizes That Mass Market Products Are Uncontrollable And Should Be Exportable

U.S. export controls still ignore the realities of mass-market software and hardware distribution. Mass-market hardware manufacturers and software publishers sell products through multiple distribution channels such as OEMs (i.e., hardware manufacturers that also 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, BSA 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.

Uncontrollable products at 56-bits cannot suddenly become controllable products at 128-bits. The SAFE Act recognizes as a fundamental proposition that the United States should *not* try to control the export of something that is, by its very nature, uncontrollable. Trying to control the uncontrollable squanders the limited resources of companies trying to comply with unrealistic export controls as well as the resources of the government as it tries to enforce unenforceable export controls, undermining the credibility of the entire system of export controls.

The SAFE Act Permits Exports Of Custom Software And Hardware

The SAFE Act ensures that if strong encryption products have been permitted to be exported to foreign banks, then custom software and hardware with comparable encryption capabilities should be exportable to other foreign commercial purchasers in that country. The U.S. should not control exports of competitive custom products embodying world encryption standards. Note that the type of software and hardware we are talking about here is a "custom" product (if it were generally available it would not need an individual license under the bill's other provisions).

THE ADMINISTRATION'S CONCERNS ABOUT THE SAFE ACT IGNORE LEGAL, TECHNICAL AND MARKET REALITIES.

The Administration Took The First Step Towards Developing A Sensible Long-Term Encryption Policy, But They Still Have Not Gone Far Enough.

The BSA members welcome the Administration's efforts to relax export controls on select products used by select users. We especially appreciate 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 communica-

tions 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. Ultimately, any truly successful, sensible encryption policy 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 a strong defense, for protecting the privacy of citizens and for preventing crime.

The SAFE Act Is Entirely Consistent With U.S. Obligations Under The Wassenaar Arrangement

Please do not be fooled by any claims from the Administration that the Wassenaar Arrangement is the multilateral agreement to restrict strong encryption that they have been touting was just around the corner for the past several years.

The Wassenaar Arrangement is a non-binding agreement among 30 countries to report on their sensitive exports that has not been approved by Congress; therefore, there is nothing requiring Congress to comply with the Agreement. Also, many countries, such as Israel and South Africa, who export strong encryption are not signatories to the Arrangement.

Regardless, the SAFE Act is still consistent with its terms. The countries agreed to decontrol all 56-bit encryption and 64-bit mass market software and hardware with encryption and to permit, *but not require,* participating countries to restrict exports of encryption stronger than 64-bits. They also agreed to remove any reporting requirements—the sole official means for actually monitoring what countries are doing.

The Administration already permits certain categories of strong encryption to be exportable under a license exception after a one-time review. The SAFE Act merely adds strong, mass market encryption products to these categories by permitting exports of such products under a license exception after a one-time, 15 day technical review.

We are skeptical that countries will individually control 128-bit encryption or do anything more than technically comply with the Arrangement, while still permitting easy exports of strong encryption. 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.

The SAFE Act Provides For Continued Export Controls On Encryption Products

The SAFE Act only relaxes export controls on encryption products that are "generally available" in the commercial marketplace and custom products if they have been approved for use by foreign banks or are commercially available from foreign companies. It does not eliminate export controls on military application encryption products. Under the SAFE Act, encryption products are "generally available" if they are widely available for sale to the public (*i.e.,* sold over the Internet, through a telephone transaction or at retail selling points), are not specifically tailored for specific purchasers or users and do not require further substantial support by the supplier for installation except for basic help line services. Thus, the SAFE Act's definition of "generally available" consists of the same elements required for 56-bit encryption software to qualify for mass market treatment under the current Department of Commerce's regulations.

The SAFE Act Ensures That Americans Can Manufacture, Buy, Sell Or Use Any Type Of Encryption Domestically

The SAFE Act explicitly affirms that Americans can sell or use any encryption domestically. It does nothing to inhibit the development of key recovery for American consumers or corporations. As I stated before, consumers are demanding and we are developing and selling them recoverable products.

It is disingenuous to state that restricting the government from mandating the use of key recovery type products, except for the government's own internal uses,

and preventing the government from requiring American citizens to use recoverable encryption if they want to do business with the government will somehow "inhibit" the development of key recovery. It only "inhibits" the government from using its great powers to effectively force American citizens to use a government approved type of encryption.

Thus, the SAFE Act importantly provides statutory prohibitions that prevent the U.S. Government from achieving domestic controls on encryption through regulation or other governmental powers which it cannot otherwise achieve legislatively.

The SAFE Act Maintains The Status Quo On The Administration's Powers Under The International Emergency Economic Powers Act, The Trading With The Enemy Act, And The Export Administration Act of 1979

The SAFE Act permits the President to stop exports to terrorist nations and to impose embargoes on certain countries under the Trading With The Enemy Act, The International Emergency Economic Powers Act and The Export Administration Act. It also permits the Secretary of Commerce to stop the export of specific encryption products to specific individuals or organizations in specific countries if there is substantial evidence that such products will be used for military or terrorist purposes. The SAFE Act, however, does ensure that the President may not use his authority to further extend encryption controls beyond those contemplated in the SAFE Act.

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.

Mr. TAUZIN. Thank you very much.

We are now pleased to welcome Mr. Tom Arnold, the Vice President and Chief Technology Officer of CyberSource Corporation, San Jose, California.

Mr. Arnold, you have got a mike coming the other way.

STATEMENT OF THOMAS ARNOLD, VICE PRESIDENT AND CHIEF TECHNOLOGY OFFICER, CYBERSOURCE CORPORATION

Mr. ARNOLD. Good morning, Mr. Chairman and members of the committee. Thank you very much for the opportunity to speak to you today.

In general, I think you will hear a slightly different story from me, not being a provider or a developer necessarily of encryption products, not being an exporter of encryption products in the industry.

We are a very small and emerging company right now, and we specifically provide real-time electronic commerce transaction processing services to Internet merchants. We are in the very heart of what is happening in electronic commerce today on the public Internet.

Specifically, just and very briefly, our services today include global payment processing, we process in 115 currencies today; fraud prevention and detection, which is a major issue for us that I will tell you several things about today; tax calculation; export compliance rules for our merchants; territory management; and delivery of both physical and digital products.

We were founded in 1996 and actually began our existence as software.net which is now beyond.com as a merchant selling software.

And I am struck by a very fond reminder that in 1994, when software.net began, we opened our doors in November 1994 believing that we had the greatest little software store on the entire public Internet and suddenly realized by February 1995 that our Inter-

net fraud rate was well over 30 percent and growing rapidly. We were rapidly going out of business.

And we immediately realized that when you open a store in the public Internet, it is totally global. You are in the best and the worst of neighborhoods simultaneously. So I am coming here today also representing the software and information industry association, and we are very strong supporters of H.R. 850.

Today's CyperSource Corporation, we process transactions for over 400 merchants on the Internet and have generated over 5.8 million transactions specifically. I don't have the revenue number for the merchants themselves, but that is the number of transactions that have actually been processed since the Internet—Christmas in 1998. So we see an extreme ramp-up coming up.

My own background spans both technology and law enforcement fields. I actually began as a patrol officer, working in the city of San Francisco, and moved my career into law enforcement computing very quickly, so I do have a background in those areas as well; and then on to NASA Ames Research Center and Silicon Graphics and then CyperSource.

Let me open by stating that the environment for electronic merchants is wrought with issues and challenges; and, like any community, the Internet population includes its fair share of criminals, including crackers, frauds, industrial terrorists, spies and professional and casual hackers.

The Internet is a very convenient and expensive medium for someone to go into as far as business, but it is absolutely wrought with risks, including the issues of consumer privacy. So how do we look at using encryption devices? How does my company use encryption today?

First, we use it to authenticate, authorize and audit for transactions coming from a merchant site. These messages help us identify who is making a request for a transaction to take place.

Integrity is a major issue. Integrity verifies the fact that the message has not been tampered with and can also be related to the fact that a message is not replayed against a merchant's site. A very common malicious denial of service attack is to attack messages in flight, replay them against a merchant site; and in a matter of minutes you have taken the merchant out of business entirely because this site cannot handle the traffic that is suddenly hitting his business.

Privacy is the most widely recognized use of encryption and has been discussed by my colleagues on the panel here today, and it involves scrambling the communications in order to conceal business information and the confidentiality of consumer data, which are the two key points I would like to stress here, the business information and the consumer data.

Nonrepudiation is another issue that we use for—or another use for encryption, if you would. And nonrepudiation is a mechanism by which the sender of an electronic message requesting something to take place cannot later deny in fact that they sent us the message and asked us to perform a transaction.

Finally, there is intellectual property protection. And I was struck by a news story and I have included it with my written testimony which I hope will be added to the record. And, in fact, it

was a news story out of the San Jose Mercury News that I was reading here on the way here describing the Dark Net and the fact that copies of those, the Star Wars film, are readily available for download right now off the public Internet through the dark sites that are out there already.

So protection of intellectual property is extremely important, and using weaker encryption all the way through hardened encryption I think are mandatory in this area. For instance, weaker technologies can be used to protect a software markets newsletter, where the life of a newsletter itself or the information that is being protected may only be 24 hours in time. But much stronger encryption is required to protect and water-marking is required to protect intellectual property or material like music or videos that may last for 5 to 10 years.

So what are the types of the things that we have seen out there in our short lives as a business here in processing transactions? We have seen this use of competitive and market information. We have watched as merchants look at other merchants' information on the Net and try to figure out what is going on. There is the threat of theft of private sales information going on, where transaction information from specifically public companies can be watched and viewed to determine if they are about to achieve their results. You can imagine the stock trading implications as a possibility here. There is theft of products and intellectual property. Then there is identity theft, which is the theft of consumer information, which is specifically the method that was used to attack our little software store when we first started, people masquerading as another person.

Many of us in this room today, our identities could be being used right now on the public Internet. Our credit card information could be being used, and transactions could be produced as though they were us. And, in essence, on the public Internet, nobody knows you are a dog.

Attacks by hackers and crackers—and one recent attack includes a hacker acquiring information to an on-line transaction where a real consumer had just completed a transaction requesting a product to be shipped. The hacker then went back into the system as that consumer and merely changed the shipping address. The product was shipped by the merchant, thinking it was going to a changed shipping address, and the consumer was billed but never received the product.

Okay. These types of attacks are absolutely nothing new. Twenty-three years ago while I was working as a patrol officer I responded to petty larceny, burglary and grand theft calls; and today there is hardly a law enforcement presence that can effectively address the daunting challenge of the global Internet.

I was actually speaking to a hacker who was stealing software, and we were trying to prosecute and locate him. And they love to flaunt their capabilities out there in the net, and he made a statement to me that has always stuck with me and, that is, basically he stated that he was driving a Ferrari on the Internet superhighway, while the cops were driving broken-down bicycles.

In a nutshell, merchants need full access to cryptographic technologies without any mandatory key escrow or key recovery sys-

tems to protect us. I am struck by the level of access that a lot of hackers have to both public and private systems specifically, and I am struck by the concept and the amount of effort that it would take to protect any sort of key escrow or any sort of recovery system in place related to these business transactions. It would be absolutely catastrophic if our private keys were compromised without our knowledge of the compromise of the keys.

I can imagine the Fort Knox-like facility that would be required to store this information and the huge infrastructure required to store the data on the keys for these transactions; and the reality is, as my colleague on the panel had stated earlier, the sites are available today from the download of hardened encryption products.

Let me leave you with one other thought. On the Internet, the hackers are going a little bit deeper underground as it stands right now.

Mr. ARNOLD. There are now "Dark Nets" that are showing up. These are private hacker networks and "warez" is a term that is used as the tools that the hackers use. They have crypt-analysis tools. They have cryptographic tools. They have password and network cracking tools that are available there.

As long as you are willing to donate a new tool or a new technique or some passwords to the site, they will grant you access to the dark site and will allow you to begin downloading the products for use for your own nefarious gains.

So let me leave you with a closing remark that—first off, thank you very much for allowing me to speak to you today. My written testimony goes into much greater details, and I would strongly urge the committee and the Congress to pass the SAFE Act. Thank you.

[The prepared statement of Thomas Arnold follows:]

PREPARED STATEMENT OF THOMAS ARNOLD, CHIEF TECHNICAL OFFICER AND VICE PRESIDENT, ENGINEERING, CYBERSOURCE® CORPORATION

Good morning, Mr. Chairman and Members of the Committee. Thank you for the opportunity to speak with you this morning about this important topic.

My name is Tom Arnold and I am the Chief Technical Officer and Vice President of CyberSource Corporation based in San Jose, CA. CyberSource is a developer and provider of real-time e-commerce transaction processing services. Our products and services offer solutions to online merchants for global payment processing, fraud prevention, tax calculation, export compliance, territory management, delivery address verification and fulfillment management. Founded when electronic commerce was just beginning to flourish, CyberSource has become a leading provider of e-commerce solutions for businesses all around the world.

I am pleased to be testifying this morning on behalf of the Software & Information Industry Association (SIIA), the result of a merger between the Software Publishers Association and the Information Industry Association. SIIA represents 1400 member companies engaged in every aspect of e-commerce and strongly supports H.R. 850, the Security and Freedom through Encryption (SAFE) Act.

Let me begin briefly by describing our company's background and my experience in developing and supporting electronic commerce on the Internet and cover the primary uses and issues related to the open and free use of cryptographic technology.

CyberSource Corporation commenced Internet commerce service operations in March 1996, as a division of Software.Net (now Beyond.com), a Web site selling software products that could be downloaded on-line or purchased for traditional physical delivery. While Software.net was on the cutting edge of an exciting trend, it faced the challenge of fraud, identify theft, product theft and a host of similar problems. Within a few months of opening the online store, the number of fraudulent credit card transactions surged beyond 30% of Software.net's total transaction vol-

ume. It seems online thieves were stealing individual identities from various Internet sources, then masquerading as the person and using the credit card associated with the identity to steal software and other products. The primary problem was examining the information provided by a consumer and determining immediately if this person is who they claim to be.

CyberSource has since expanded its offerings to a full suite of electronic commerce transaction processing services, which today include on-line payment processing; advanced fraud detection and screening technologies; export screening; distribution control; sales and VAT tax systems; and, digital product deliver systems (software, music and video download technologies).

Today over 400 merchants have chosen to use CyberSource, generating millions of transactions per month.

My own background spans patrolling the streets as a police officer to implementing some of the early law enforcement computer systems for the State of California. I have worked at NASA Ames Research Center, designed and built the first e-commerce platforms at Silicon Graphics Corporation, and designed the systems for CyberSource Corporation.

Privacy and Security are Critical Factors to the Success of e-Commerce

Let me open by stating that the environment for electronic merchants is wrought with issues and challenges. The Internet is first and foremost a global community and provides a huge opportunity for merchants to offer the products and services to the broadest possible community of potential customers. Unfortunately, the Internet population includes its fair share of criminals, including but not limited to hackers, crackers, frauds, industrial terrorists, spies, and even casual hackers.

It is clear that without the ability of companies like mine to protect the privacy and security of online consumers and merchants, e-commerce will not flourish. While the Internet is a convenient, inexpensive and increasingly popular medium, companies and individuals cannot afford to take advantage of the benefits of the Internet. Simply put, no amount of price competitiveness, convenience or marketing will entice an online consumer if they fear that their privacy and security will be compromised.

To foster the confidence needed to ensure that e-commerce continues to grow, encryption is vital. In short, cryptographic technology is used to protect e-commerce transactions in five major functions:

(1) Authentication, authorization and auditing: This is a method for identifying who is making a request, authorizing access or capabilities, and tracking what action is taken.

(2) Integrity: This refers to verification that a message is intact; that the message was not intercepted and tampered with; or, that the message has not been replayed (a common, malicious denial of service attack that can put merchant out of business in a matter of minutes).

(3) Privacy: This is the most widely recognized use for encryption technologies. It involves scrambling the nature of the communication or data so as to conceal business information, ensure privacy of consumer data, conceal financial or payment information, and protect product and pricing information.

(4) Non-repudiation: In the virtual, electronic world, this ensures that any initiated message cannot later be repudiated by the sender of the message. In essence, by guaranteeing that the keys used to generate the encrypted message are certified and remain in the sole control of the sender, and that no keys can be derived through a recovery process that has been attacked, the sender cannot repudiate that they initiated the message. This is a very important concept and is at the heart of electronic commerce.

(5) Intellectual property protection: This includes a spectrum of cryptographic technologies that protect downloaded products to applying digital water-marks. The level and use of hardened encryption versus weaker encryption is directly related to the useful life of the product being protected. For instance, a weaker technology may be used to protect a stock market newsletter that will be out of date by the next morning, while hardened encryption and watermarking might be applied to a piece of music that might have life of five to ten years.

Under the current encryption export policies, we are generally allowed to license the weaker 56-bit encryption methods for export, and for certain financial information like a customer's credit card number, we may be allowed to use strong encryption in limited markets. However, our inability to use robust protection throughout the e-commerce sales process unfortunately places our merchants, manufacturers, and distributors at risk.

Encryption Export Restrictions Place US Companies at Competitive Risk

Competitive information, products, and information about customers and their transaction are at risk without strong encryption products to provide security and protection. Foreign competitors, beyond the reach of US law, have full access to hardened encryption technologies. Here is a brief list of the risks today:

(1) Consumer information can be acquired by competitors and used to attack markets.
(2) Transaction information about products being sold and the number and size of orders being received. This information could be used, for example, to make stock trades by determining if a public company is going to achieve its sales goals at the end of a quarter.
(3) Products and intellectual property.
(4) Consumer identities acquired by a hacker and used to commit fraud.
(5) Products and valuable intellectual property that is acquired and posted on dark nets. While flying to this hearing, an article in the local San Jose, California paper stated that pirated copies of the new Star Wars films were already available on-line.
(6) A list of ever changing attacks by hackers and crackers. One recent attack involved hackers acquiring access to an on-line purchase transaction. This data was used by the hacker to contact the merchant and have the merchant change the shipping address. By the time the problem was discovered, the thief was long gone.

There is nothing new in these types of attacks on businesses. Twenty-three years ago, while working as a patrol officer, I responded to petty larceny calls, burglaries, and grand theft. Today, there is hardly a law enforcement presence that can handle the global Internet environment. I'm reminded of a comment made to me by one hacker flaunting his accomplishments when he stated that he was driving a Ferrari on the Internet super highway, while the cops were on broken down bicycles.

In a nutshell, merchants need full access to cryptographic technologies without mandatory key escrows or key recovery systems to protect themselves. Think of these as the deadbolt locks or the alarm system on our electronic business.

Encryption Protects a Wide Variety of Information

I fully respect the needs of the Justice Department and our law enforcement agencies to protect US citizens and interests from domestic and international threats, from criminal activity, and from terrorist acts. Unfortunately, it is clear that the current encryption policies restrict only law abiding companies and individuals since cryptographic and encryption technology is freely available on the Internet. Additionally our foreign competitors routinely use hardened encryption.

Encryption can be used to protect a wide variety of information, sensitive data and transactions. While the need for encryption has greatly increased with the growth of online commerce, computer systems of all types rely on encryption to provide privacy and protection. Encryption is used in network operating systems, communications software and hardware, data storage products, and even in common products like word processors or spreadsheets. Encryption is an incredibly useful technology, and high-tech companies and their customers need to be able to use the most robust tools available to ensure that their information is secure.

For online companies, encryption restrictions erect a daunting barrier to the expansion of markets. As e-commerce grows, online companies are offered a tremendous opportunity yet are denied the ability to fully take advantage of this shift in the market. More importantly, however, encryption provides companies a means to protect their products in ways that can help prevent misuse by even the most determined of software thieves.

To complicate matters even more, hackers and crackers share their "warez" (tools) throughout the public Internet and through "Dark Nets" (private hacker networks—something like a private club where new members have to share some new "ware" to gain entry). Some of the tools on these sites include: crypt-analysis tools, cryptographic tools, password cracking tools, network cracking tools, stolen passwords to sensitive networks and sites, and full technical information on using the tools. In one case, a major telecommunication companies own systems were attacked, and used by hackers to host a illegal "warez" site for several months. The hackers were freely delivering stolen products, credit card numbers, credit card generators, personal information on people who threaten the hacker world, and information on breaking into numerous sensitive and critical computer systems.

The strong encryption key recovery or key escrow schemes being proposed as middle-ground are inherently insecure and must be strictly administered. I'm sure members have heard stories about hackers who use strong encryption to scramble data files on their machines, thereby thwarting law enforcement investigations.

What may not have been explained is where the hackers obtained the encryption technology and, further, the level of access to sensitive systems. Between 1993 and 1995, a couple of key hackers being pursued by the FBI access to: cellular networks, public telephone taps, ability to access private email accounts and files. In many of these cases, the hackers used social engineering techniques to get people in sensitive positions to voluntarily allow access this information and capabilities.

It is extremely naive to believe that key recovery systems or key escrow cannot and will not be compromised, either through insider abuse or external penetration. I can think of little worse than the undetected lose of private encryption keys from our systems or any merchant system. The business impact would be catastrophic. In response to this type of threat, any government funded and mandatory key recovery or escrow system would surely have to be secured on the scale of Fort Knox, or the level of security required to protect our Country's most valuable assets. Surely it would be hardly cost effective for the number of electronic wire-tap orders where a key would be recovered and information monitored. I doubt seriously that any hacker, criminal or terrorist would use recoverable encryption technology when strong, unrecoverable encryption is available on the Internet or Dark Nets.

For this reason, the use of recoverable encryption and key escrow technologies need be voluntary and under the complete supervision of the user.

In conclusion, I'd like to highlight that the Internet community offers a great opportunity for merchants. The Internet Christmas shopping season of 1998 proved the viability of this marketplace, Christmas 1999 promises to be even better.

As these new opportunities develop, Internet merchants make substantial investments in new computer systems and technologies to help them address the growth. The advertising outlays to attract new customers is also substantial. It may take as much as $128 to get a single consumer to press the buy button.

The risks for merchants in this growing segment of our economy from the loss of critical business information and private consumer information is extremely high. A major manufacturer of computer hardware estimated their loss from theft that resulted from fraud and compromise of proprietary consumer information is 7% of their annual revenues and is growing faster than sales.

Merchants need open access to strong encryption to protect their investments, technologies, products, and consumer information. As new payment or merchandising technologies are implemented, hackers and information mercenaries will develop tools to attack these technologies for their illicit gain. For these reasons, we fully support the Security and Freedom Through Encryption Act and urge its prompt passage.

Thank you.

Mr. TAUZIN. Mr. Arnold, thank you very much. Indeed, your written testimony is very illustrative of all of these problems on the Internet. Thank you for that.

I might mention to you that you are correct about on the Internet no one knows whether you are a dog. A newspaper in Louisiana successfully registered four dogs to vote in Louisiana. I don't know whether they were blue dogs or yellow dogs.

Somebody else that I mentioned—remember we took up WIPO? I think "Titanic" had just been down loaded on the Internet that same week. So we have seen this over and over again. But, of course, if the critics are right about "Star Wars," it might not make a whole lot of difference.

Dr. Gene Schultz, trusted security advisor of Global Integrity Corporation of West Lafayette, Indiana. Dr. Schultz.

STATEMENT OF E. EUGENE SCHULTZ, TRUSTED SECURITY ADVISOR, GLOBAL INTEGRITY CORPORATION

Mr. SCHULTZ. Good morning. I work for Global Integrity Corporation, which is a wholly owned subsidiary of SAIC, Science Applications International Corporation. It is a very large consultantcy. It is international in nature. I am not here to represent the interest of anybody who makes any encryption product. I hope they make a lot of money in their endeavors, but that is not why I am here.

I am here to speak my conscience. You see, I have an unusual background. I have been in the trenches there, and I see what is going wrong in computer security. I started and managed for 4 years the U.S. Department of Energy's incident response team called CIAC.

After that period of time, I worked out with industry when I was at SRI consulting down in Menlo Park, California. We worked with some of the largest corporations, not only in the United States but in the world.

I have been a witness to over a thousand different security-related incidents in the computer security area. I have seen what breaks down. I have seen what goes wrong. I have worked with law enforcement. I know many people in the law enforcement community.

And if you read books such as "At Large" by David Freedman, you will see some of the details of what really goes wrong. What really goes wrong isn't that some bad guy goes out and uses encryption against you or anything like that. It's hard enough for this community to deal with the evidence that is at hand in clear text.

I would like to, therefore, switch the topics just a little bit to the area of technology itself and tell you that what we have out here in the area of networking isn't what we had 2 or 3 or 4 or 5 years ago.

What we have in terms of telecommunications networks, in terms of computer networks, are considerably more complex now than they were just even a few years ago when encryption or restrictions certainly were considered a very, very reasonable thing to have.

You see, today somebody from a major vendor company said that the network is the computer, and that's really true. Today's computers aren't these stand-alone computers that sit on desk tops, and whether or not you have encryption may not make that much different because you can control who gets those computers by locks, keys, guards, and guns.

Today's computers are really meant to interface with networks. In fact, sometimes they don't work so well if they are not interfaced with a network. In addition to that, when you set up a computer now, you are opening up the possibility that somebody from potentially anywhere in any part of the world could possibly make a connection to that computer.

Your computer could be connected to people from Hong Kong, from people from Beijing, people from Melbourne, Australia, and on down the line. There are no distinct boundaries in networks anymore.

It used to be that we had a nice little ARPNET and that split into what was called NSFNET which we call the Internet and MillNet.

But it's not like that anymore. In fact, networks are largely in control of people who are Internet service providers. Metropolitan area networks, they are regional networks tied together through some massive backbone kind of structure.

Even the Internet as we know it now is rapidly breaking down. You see, it is too slow. It doesn't meet our purposes very well. And

vendors are developing new networks that will supersede and far by pass network. We don't really have control over this technology as it proliferates.

In addition to that, I don't need to be very smart to attack a computer off the network. I just need to download a program from one of the dark sites that Mr. Arnold talked about, or one of many others, and simply startup a program and it does things for me.

And so I can be older or younger. It is not true, by the way, that hackers are all young people. There are many older and experienced hackers out there. But the state-of-the-art of attacking networks, it has been proliferating over the last few years, much above when, again, we were first concerned about the problem with encryption control.

Network services you get—web services for file transfer services generally demand no or at least little identification. And probably the worse threat to corporate America today from my experience is somebody planning a network capture devise that captures the traffic that goes through the network and grabs the memo that goes from the CFO to the CEO or the CEO to the CIO.

And because of that—and people don't realize it. They think that it is external hackers that are trying to get you. But the real threat in which encryption technology can protect you lies from within your own organization itself.

Finally, I would say that networks are radically different in that now transactions occur over networks in which it is possible to repudiate transactions. No, I didn't buy this; don't bill me this. But you keep whatever goods or services have been shipped to you.

I have seen some pretty bad incidents. I was one of the principal observers of the break-ins into U.S. military systems during Operation Desert Storm and Desert Shield. I saw people from foreign countries break into U.S. computers with impunity.

Had we had a better level of encryption practiced during that time, we could have virtually stopped the bad guys from getting information about, for instance, our munitions movements in the Middle East, about what battleships were moving overseas, how many troops were going from which Army base here in the United States over to which destination.

Now we can say, well, yes, that is all within the government. But the fact is encryption technology was not that advanced in terms of its actual deployment at that time.

I have seen a company recently that had somebody try to break in, did break in, to their network, got into a machine, attempted to initiate a $20 million financial transaction. Fortunately they failed.

Better cryptology could have addressed that problem and should have addressed that problem, but it was not in place. Frankly, that corporation was lucky. I saw another corporation in which somebody did break into their network. They did transfer files with impunity. The financial loss is immeasurable. Many of their pending copyrights were transferred off to some unknown location.

In this particular case, again, encryption could have made a big difference. I have seen network capture devises used against corporations where people have captured virtually everything out of a major corporate network.

Again, encryption could and should have helped address this problem also, in the telecommunications arena. Don't think that the only danger is the Internet. We have lots of PBX to Internet, PBX to private networks kinds of links.

In those arenas, again, voice goes across in clear text, voice conversations between a CEO and critical business partners. We don't use encryption sufficiently because we have too many barriers on that encryption.

We don't have sufficiently strong encryption. And you can't fool industry. If they know that somebody is faulty, they are not going to invest the money in it. We know also that the industry has to put up with the least common denominator.

They know that the third party business partners are out there with weaker crypto. They are going to have to lower their crypto capabilities to this weaker capability if they are going to maintain encrypted links. Therefore, often they do not.

Finally, something that has not come out, I believe, up to now. I believe that the U.S. Government is sending a strong negative message to industry. I think they are saying somehow that there is something wrong with this technology, that somehow there is something not very good about it.

It is something that, gee, well, maybe pedophiles, terrorists, criminals, and all of this are associated with it. I think that industry is very quick to see that if the government is not giving it a green light, that it is going to be slow to deploy it.

What we have, in effect, is a situation where we have an arid land. We desperately need water, but we are afraid that the outlaws are going to get the water, so we poison the well. I think that is what happened. Maybe that worked 5 years ago. Maybe that worked 10 years ago. But today technology has changed.

We have to come to grips with the changes in technology. We are, in fact, worse off now in protecting our critical national infrastructure than we were 3, 4, 5 years ago. Technology has advanced that far, but the ability to use encryption has not. I strongly urge you to pass the SAFE Act.

[The prepared statement of E. Eugene Schultz follows:]

PREPARED STATEMENT OF E. EUGENE SCHULTZ, TRUSTED SECURITY ADVISOR AND RESEARCH DIRECTOR, GLOBAL INTEGRITY CORPORATION

NEW DIRECTIONS AND OPPORTUNITIES FOR CRYPTOGRAPHY

ABSTRACT

This paper addresses the issue of U.S. cryptographic restrictions. Committees in both the U.S. House of Representatives and Senate are considering legislation that relaxes these restrictions. The main reasons for closely guarding cryptography (i.e., protecting U.S. military and law enforcement interests) have *historically* been legitimate. They now, however, constitute considerably less justification for keeping these restrictions. Networks and the computing systems that connect to them are now much more complex; they are thus more subject to a myriad of attacks. Networking itself is an integral part of the U.S. critical infrastructure. The use of strong cryptography in securing these networks is now virtually a necessity in controlling against attacks and misuse such as stealing files from remote systems, preventing perpetrators from stealing plaintext message traffic containing valuable information and passwords, and proving that someone who initiates a financial or other kind of transaction has indeed done so. Strong cryptography is also equally necessary in the telecommunications arena, in which valuable data also traverses telecommunications links. The current U.S. policy on cryptography has played a major role in

the commercial sector's inability and unwillingness to deploy it where it is needed. The result is substantially elevated security-related risk within critical sectors (e.g., financial services and hospitals) within the commercial world. The fact that the U.S. Government has also sent a distinct, negative message to the U.S. commercial arena concerning the use of cryptography is perhaps the most serious of the obstacles the Government has created. Equally disturbing is that the current U.S. policy will eventually ensure that the U.S. loses its leadership in the cryptographic arena. It is thus now time to change the U.S. policy on cryptography by relaxing current restrictions.

Background

What should the U.S. do about its policy concerning cryptography? Should, as several key agencies of the Government argue, cryptography continue to be restricted to the same degree that it has been in the past, or should it be more freely available, both within the U.S. and internationally?

Not surprisingly, polarized positions have emerged. Proponents of restricting cryptography argue that doing so is in the best interests of national security in addition to law enforcement needs. Hostile foreign powers and criminals who have access to powerful encryption can use it in potentially harmful ways—to maintain a secrecy of communications that U.S. interests cannot tolerate, store evidence in a form that cannot be deciphered by anyone but themselves (and thus in a form that is unusable to law enforcement), and so on. Those who advocate these restrictions also propound that cryptography is currently not sufficiently cost-effective, useable and manageable to justify the risk of making it more freely available.

This paper advocates a different position—that whereas U.S. restrictions on cryptography may have made sense in the past, they are no longer appropriate as is. They need to be eased.

Changes in Security-Related Threats

The computing world has shifted focus considerably during the last decade. Whereas a reasonably large proportion of computers was still standalone one decade ago, now it is rare to see a standalone computer. The computing as well as the telecommunications world is massively networked. Networks are extremely difficult to defend from attacks for several important reasons:

- Today's computers are considerably more sophisticated than they were a decade—even a half decade—ago. Today's computers are in fact built for networking. Virtually anyone—friend and foe alike—can obtain one or more of these computers and utilize network services. Unfortunately, this also means that virtually anyone can perpetrate attacks over networks.
- Networked computers are in most respects a bigger target than computers that do not connect to one or more networks. Depending on how a network is configured and a large number of additional factors, it may be possible for anyone in any part of the entire world to be able to remotely reach a given computer, and thus to attack it.
- Where networks start and where they end are both nearly impossible to determine. In general, it is difficult to defend something that has a well-defined boundary.
- The state of the art for attacking computers over networks has evolved dramatically over the last few years. Many software programs that allow even the most naıve of computer users to launch powerful attacks over networks are now freely available over the Internet as well as through other sources.
- Networks offer services that typically demand little or no identification of the people who utilize these services. Avoiding being identified is usually trivial for network attackers. Being anonymous over the net emboldens network attackers.
- A perpetrator who has access to one point in a network between a computer from which someone sends a message or a file and the computer on which someone receives it can capture traffic that is sent. By default, all such traffic is in plaintext, meaning that whoever captures it can read it right away. Privacy over networks is thus a major concern.
- Networks make electronic transactions possible, yet dishonest people can order goods and services over the net, then deny ever authorizing the order.

My experience in the world of computer security spans nearly 15 years. During this time I have been faced with many challenges and seen many eye-opening experiences. One of the most startling sets of experiences occurred nine years ago when intruders from the Netherlands broke into U.S. military computers with impunity, stealing information about weapons systems, U.S. troop movements, ordinance shipments, and so forth in the midst of Operation Desert Shield and Operation Desert

Storm. The U.S. military community had the cryptography available to protect the sensitive information that the intruders stole but did not use it.

Approximately five years ago a small number of perpetrators installed software programs that captured network traffic that went through Internet service providers throughout the U.S. The main target (although not the exclusive target) was passwords—the perpetrators used the passwords they captured to break into the computer accounts of tens of thousands of users, mainly in the U.S.A., but also in other countries. The perpetrators obtained so many passwords that they were not even able to use a significant proportion of them during the time span in which the attacks occurred. Encrypting the traffic that went into and out of the Internet service providers' computers would have prevented these attacks.

I recently helped a client corporation respond to what was a very potentially serious attack. The client has a number of networks, one of which contains computers that initiate and control major financial transactions. Someone, apparently not a company employee, obtained access to this network through a connection with one of the corporation's business partners, then attempted to initiate a multi-million dollar financial transaction. Fortunately for the corporation, the attacker did not know quite enough about the procedures for initiating such transactions and thus failed. Use of cryptography that strongly assured the identity of the person who initiates these transactions would have considerably lessened the probability of success in this scenario.

Another corporation was not so fortunate. A remote attacker broke into one of a corporation's networks and transferred many proprietary files to another computer that the attacker had taken over. The exact amount of financial loss remains unknown, but it is not unreasonable to think in terms of tens of millions of dollars. Had the stolen files been encrypted with strong cryptography, they would have been of no value to the attacker and the people to whom he undoubtedly sold them.

The fear of attacks such as breakins into computing systems often overshadows concern for other types of attacks. In reality the potentially most devastating attack in the corporate world is one in which someone plants a device or software program that captures all the network traffic that goes by a certain part of the network. The attacker can capture not only passwords, but also critical data files, messages sent between corporate officers, and a variety of other sensitive and valuable information. This information is almost without exception transmitted in plaintext. Indeed this kind of attack occurred several years ago at the headquarters of a major manufacturing corporation. Perpetrators planted a device that captured all incoming and outgoing network traffic. Luckily, someone discovered the plot to capture and sell corporate information before the perpetrators were able to sell it. Again, the use of cryptography to prevent plaintext traffic from being sent over this network would have deterred the perpetrators from carrying out this kind of plot in the first place.

Computer networks are not the exclusive targets of attack; telecommunications links are also vulnerable to being tapped. The corporate PBX is a particular target. The fact that voice and data traffic is by default sent in plaintext over many telecommunications links is once again a cause for major concern. Unbelievably, some organizations encrypt network traffic but do not encrypt traffic that moves through telecommunications links, even though these links feed into the computer networks and vice versa.

Why Restrictions on Cryptography Serve as Obstacles

In today's hearings we will once again be reminded of reasons for restricting cryptography and why, if and when restrictions are relaxed, we will have reached what some will call a dramatic, irreverseable point in U.S. ability to maintain control of cryptography. On the surface, these views make sense, but they do not make as much sense now as they did two or three years ago. The problem with the logic of these views today is that (as discussed previously) networks are now so much bigger, more complex, and more pervasive. Corporate America is now considerably more reliant on computer networks than it was only a few years previously. And, with a few notable exceptions (mainly in the banking and financial services arena), corporate America is not deploying cryptography to a great extent. Why? Several reasons stand out among the primary probable causes:

1. Cryptographic presents a myriad of practical difficulties, including the problem of cryptographic key management and the fact that using cryptography causes slowdowns in system and network performance.

2. The financial cost of using of cryptography is still rather high. For many corporations, the benefits do not currently outweigh the cost.

3. Strong cryptography is for the most part not available to corporations, even in the U.S. With magazines and newspapers running articles about how someone else has broken one, then another cryptographic algorithm, corporations hesitate to

make the financial investment to widely deploy cryptography that they perceive may be flawed.

4. Businesses are now truly global in nature more than ever before. The fact that businesses do not exist in isolation means that a given U.S.-based corporation is likely to have offices in other countries (something that generally causes only minor complications in terms of ability to deploy encryption). More significant, however, is that fact that many third-party business partners are headquartered in countries in which U.S. cryptographic restrictions are enforced. The U.S.-based corporations are thus forced to choose between implementing the relatively weak cryptographic solutions generally available to these non-U.S. entities (to create a common encryption link with these entities) or to not deploy encryption at all. Too often the more reasonable choice is the latter.

5. Whether or not the U.S. Government realizes this, its policies on cryptography are sending a distinct, negative message to industry. On one hand, some U.S. Government agencies and institutes encourage industry to use encryption, but then others talk about the dangers of strong encryption and the harmful effects of allowing it to be too widely disseminated. At the same time elements from within the Government have publically voiced concern about the cost and performance decrements associated with the encryption that is currently available. The message to industry is that there is something wrong with encryption, that strong encryption is something that is used by spies and pedophiles, or that, even if industry uses encryption, it must understand that the "best" encryption is reserved for inner pockets of the Government. The net effect is that industry's motivation to deploy encryption has been undermined.

The most unfortunate result is that organizations such as financial service providers and hospitals that have the greatest need to use encryption too often do not use it. The U.S. Government has in effect "poisoned the well" in a desert to keep outlaws from drinking from it. Unfortunately, the nearby villagers meanwhile are dying of thirst.

Other countries are developing cryptographic technology and making it available to the rest of the world anyway. Any country (regardless of the status of its relationship with the U.S.) can obtain strong cryptography today independently of what the U.S. makes available. Worse yet for the U.S., with supportive policies by foreign governments in which strong cryptographic technology is developing and strong international demand for strong encryption technology, this technology will some day in the not-too-distant future exceed the U.S.-based technology. The unfortunate result for the U.S. is that our ability to control cryptography (a major goal of those who advocate strong restrictions) will have passed us by anyway. *Our ability to control cryptography depends to a large extent on our ability to be the leader in cryptography technology.*

Additional Pseudoreasons for Restricting Cryptography

Suppose that, as opponents of easing cryptographic restrictions often assert, the U.S. relaxes cryptographic controls, then finds that some adversarial or criminal element is using strong cryptography in a manner that is significantly harmful to U.S. interests. These opponents too often, however, fail to consider the available brainpower and resources within the U.S. available to crack the cryptography. Overlooking the impressive historical achievements of U.S. cryptanalysts in what amounts to a proactive concession of defeat—saying that the U.S. may or will not be able to cope with any fallout that strong cryptography brings should it become more widely available. Furthermore, ironically, numerous hostile foreign powers, terrorist groups, and criminal organizations almost certainly have the ability to break at least some of the cryptography that the U.S. is trying so hard to protect.

Opponents of relaxing U.S. cryptographic restrictions additionally fail to come to grips with another firmly established historical precedent of which the U.S. is all too aware (e.g., the Walker spy case). A cryptographic system, no matter how strong, is only as strong as the weakest link. The weakest link is normally a person—a greedy, disgruntled, or idealogically-motivated person who thoroughly knows the system. If the U.S. needs to crack a cryptosystem that is not technically feasible to crack, it can always attempt to crack this system by courting the people who know about and work with the system.

Conclusion

In conclusion, those who have opposed relaxation of cryptography in the past have taken a reasonable stand. The major problem today, however, is that the technology of the past is not the technology of today. Today's networking technology in particular has introduced many new, security-related threats, most of which can be addressed by today's encryption technology. Computer and telecommunications net-

working are absolutely essential to the U.S. critical infrastructure. The sectors within the U.S. that most need to deploy this technology, unfortunately, either do not deploy it at all or do not use it to its potential. *The result is that we are now worse off with respect to protecting our critical infrastructure than we were a few years ago.* This trend will become exacerbated if not reversed. Only one reasonable solution exists—to relax restrictions on cryptography as soon as possible.

Mr. TAUZIN. Thank you very much, Dr. Schultz. Compelling testimony.

Now, we will hear from a fellow that Mr. Hornstein fears so much, Mr. Holahan, executive vice president, marketing, Baltimore Technologies, from Dublin, Ireland. Mr. Holahan.

STATEMENT OF PADDY HOLAHAN, EXECUTIVE VICE PRESIDENT, MARKETING, BALTIMORE TECHNOLOGIES, INTERNATIONAL FINANCE SERVICES CENTRE

Mr. HOLAHAN. Good morning, Mr. Chairman and members of the subcommittee. My name is Paddy Holahan, executive vice president of marketing for Baltimore Technologies. I am responsible for the design and marketing of all of Baltimore's products.

I am testifying today to provide the viewpoint of a leading information security company that originates from outside the USA. I would like to put my comments in context by giving you a brief instruction to Baltimore technologies.

We are a publicly listed company on the London Stock Exchange. We develop and market commercial security products for use in business and e-commerce. Most of these products use encryption technology.

We have software and hardware development centers in Ireland, the UK, and Australia and have sales offices in 16 cities worldwide and customers in over 40 countries. Many of these customers are governments, government bodies, large corporations of some of the world's leading financial institutions.

We have business and technology relationships with many companies including U.S. corporations such as Intel, Cisco, IBM, Netscape, and Security Dynamics/RSA. While we do not develope software inside the U.S.A., we are successfully selling our products and growing our business throughout America.

We are one of the leading global security companies in the world. We export the majority of our products from the country of development. These exports are regulated by national government of the relevant country, all of which are signatories to the Wassenaar Arrangement.

Accordingly, Baltimore has unrivaled experience in operating in the most international of export regulation environments. Our business objective is to provide the world with the underlying electronic security infrastructure to support world commerce.

The underlying framework of world commerce requires a reasonable regulatory environment that transcends national boundaries. This framework has to be acceptable to the trade requirements of international governments and freedom of the individual. Encryption is now a common requirement for almost any Internet or e-commerce product.

This is in contrast to a few years ago when encryption was only necessary for specialist products. It is now clear to everybody that

the regulatory system designed to control cryptography in the past cannot be sustained into the future.

The next move is highly important, and we will encourage and support all initiatives to develop the structure that supports the requirements of industry and of governments.

The SAFE Act will completely alter the nature of the security market both inside the United States and the rest of the world. We welcome the use of cryptography for the development of a safe, secure e-commerce structure within the United States as proposed within the SAFE Act.

Security and trust are essential parts of commerce, and cryptography is an essential part of e-commerce. The prohibition on mandating key escrow will also remove a potential technological obstacle to the adoption of secure systems.

The export provisions of the SAFE Act will potentially revolutionize the worldwide international e-commerce markets. It will clear the way for full-time encryption of a vast range of security and general-purpose applications, including Web browsers, e-mail, and fine encryption.

The act will enable the vast majority of non-American corporations and consumers to conduct business with each other over the Internet using strong security. However, this unilateral move comes up soon after 33 leading countries, including the United States of America, agreed to harmonize a base level of crypto regulation in the Wassenaar Arrangement.

The SAFE Act may solve a single problem of U.S. export but may cause other difficulties in selling and using U.S. security products between other countries, as many U.S. corporations have development and manufacturing and distribution facilities throughout the globe.

This is not a U.S.-versus-the-rest-of-the-world issue. The United States is in a unique position in that it is the largest single market for development, export, and purchasing of high-technology products.

I would encourage the committee to consider a more international approach to the export section of the SAFE Act so that we recognize the international aspect of industry and of the Internet. I also wish to refute the widespread perception that non-U.S. security companies flourish solely because of inability of U.S. companies to export products with strong crypto.

As part of my research for this testimony, I was astounded by some of the claims presented to other subcommittees. It is vital that this subcommittee is not misled into developing legislation based on incorrect information. We welcome any moves to encourage open markets for encryption products throughout the world.

The current U.S. regulations may appear to give non-American companies a massively unfair advantage, but in truth the advantage gained is slight.

U.S. companies dominate in the software and technology worldwide and will continue to do so. There are tens of millions of users of Microsoft and Netscape products outside of America, most of whom have reduced-strength cryptography.

Even though freeware products exist to reinstate the strong crypto, a tiny percentage of people have done so. We derive a high

percent of our revenues from the financial sector, but U.S. companies are free to offer strong cryptographic products.

We compete successfully in the same way as any technology does, by bringing the best products to market first. I do not know of any significant non-American companies who deliberately set out to build a business based on the U.S. export situation.

The only situations we encounter of companies deliberately side stepping U.S. regulations are the international subsidiaries of American corporations. While U.S. companies are subject to export restrictions, they have a domestic market that is the most active and sophisticated in the world, comprising 260 million people.

Many of Baltimore's products emanated from our Ireland development center with a domestic market of only 4 million people. American companies are not losing the technology, nor will they.

There exist many significant impediments to the development of security products, and many American companies would cite the commercialization of various patents as being more significant. The SAFE Act presents a highly significant opportunity to change the security landscape within the United States and beyond. It will impact both U.S. and non-U.S. security and encryption companies and potentially alter the way in which e-commerce and the Internet are secured.

I would like to thank you for your invitation to present here today.

[The prepared statement of Paddy Holahan follows:]

PREPARED STATEMENT OF PADDY HOLAHAN, EXECUTIVE VICE PRESIDENT OF MARKETING, BALTIMORE TECHNOLOGIES

INTRODUCTION

The Subcommittee on Telecommunications, Trade and Consumer Protection has requested that Baltimore Technologies present testimony on the SAFE Act.

We would like to thank the committee for the opportunity to present views and assist the committee with its work. As a leading non-US originated developer of security and encryption products with sales throughout the world, including the United States of America, we can provide a different perspective on the implications of this legislation. We are not encouraging the members to vote in a particular direction.

Cryptography is being incorporated into more and more technology products every day. The general technology boom and the Internet in particular fuel this explosive increase in use of crypto. It is apparent to everyone that a regulatory system designed to apply to a small number of specialist products cannot be sustained into the future.

Baltimore Technologies is a publicly listed company with headquarters in Ireland, UK, Australia and the USA. As a leading global supplier of security products for use in enterprise and e-commerce systems, we welcome all attempts to encourage worldwide open markets for cryptographic products. As a global company, we wish to compete on a level playing field and let the consumer choose the best product and supplier.

Baltimore Technologies, along with many other non-American originated companies, has no reservations with the underlying concepts in the SAFE Act. Indeed, we would welcome the global availability of products such as browsers, secure email and emerging technologies that will encourage generate the environment for world e-commerce.

A large portion of Baltimore's business comes from customers who are free to choose products from our competitors from the USA, Canada, Europe. These customers are either American corporations or financial institutions who can obtain export licenses for US products. We believe that a very small percentage of our business comes as a direct result of American export restrictions.

Baltimore has technology and business relationships with many world-leading technology companies. These relationships are based on mutual business benefits

and not because Baltimore is a non-US company. In the past three years we have worked with companies such as Intel, Cisco, IBM, Security Dymanics/RSA, Netscape. These relationships exist both inside the United States and in other countries where Baltimore operates.

(A) Comments on SAFE Section 2: Sale and Use of Encryption

As a growing supplier of security and cryptographic products within the USA, Baltimore Technologies welcomes the provisions of section 2 which ensure that businesses and individuals will continue to have the right to buy and use security products for legitimate personal or business use.

The prohibition on *mandatory* key escrow is also welcomed. Key recovery has certain legitimate uses in commerce and it remains an important *optional* security system for certain industries.

(B) Comments on SAFE Section 3: Exports of Encryption

Baltimore Technologies does not develop products in, nor re-export products from the USA. As such the provisions in the SAFE Act will not change the manner in which we do business—but it will completely change the way US companies compete in the global market.

In considering liberalising cryptography export policy the committee should consider the following:

1. Passing the SAFE Act will not solve all export problems for US corporations and will not create the international environment that is fundamental for world commerce. US companies develop, manufacture and distribute products from many countries worldwide. The SAFE Act will enable export from the US, but thereafter companies will have to comply with the export regulations of other countries. It is fundamental to the success of world commerce that the SAFE Act is consistent with the regulatory environment in all key world economies.

2. The US's current export stance impacts the vast majority of computer users worldwide. For example the overwhelming majority of Internet access is conducted using US products such as Microsoft Windows and Internet browsers that remain crippled at 40-bit encryption outside of the US.

3. This Act will completely revolutionise the Internet and e-commerce internationally, giving international free access to full strength secure Internet browsers and email along with a range of other products.

4. The passage of this Act may encourage other countries to bring their export regulations in line with the USA. This will create a freer market for cryptographic products worldwide.

5. Most countries have a cryptography export policy. These policies vary from country to country, but it is wrong to assume that the US is currently out of step with the rest of the world. The unique part of the US export system is the use of restricted key-lengths.

6. It is true that all security and encryption companies are prone to losing business as a result of export, import and usage restrictions imposed by national governments. It is important to recognise that US companies are not unique in this regard. The United States, as the largest exporter of software and high-technology products in the world, feels the effects of export restrictions more noticeably than other countries.

7. The SAFE Act, if passed, may contradict the terms of the recently agreed Wassenaar Arrangement signed by the governments of 33 leading nations, including the USA. While the Wassenaar Arrangement imposes unwelcome restrictions on cryptographic products, Baltimore welcomes the attempts at international consistency and harmonisation.

8. The SAFE Act correctly distinguishes between products that include cryptographic functionality and pure cryptographic products.Many technology products now include cryptographic elements in order to provide security for Internet users. These products provide functionality that is simply made secure by crypto. For example Web Browsers and conventional email systems are in widespread use, but they also include cryptography which can secure communications if necessary.

Pure cryptographic products, on the other hand, can be used in a more general-purpose manner and can be used to build a wide range of security systems for almost any use.

OTHER COMMENTARY

The US cryptography debate has generated a great deal of interest and debate, but there is much misunderstanding of the global situation.

1. It is misleading to state that non-American companies are flourishing because of the current US policy. Surveys are often presented stating the number of pro-

grams available internationally that include strong crypto (e.g. PGP, Fortify). What these surveys neglect to mention is that the dollar value of the sales of all these products is very small when compared with sales of similar products in the US. The United States dominates the world's software market and will continue to do so. While there is no argument that some US companies are obviously limited in their non-US markets for strong-crypto products, it is not the case that non-US companies are flourishing at an exaggerated rate.

2. Most countries do have effective export restrictions that regulate export of cryptographic products. Baltimore Technologies has to deal with three export administrations in Ireland, the UK and Australia who regulate encryption product exports in different ways.

3. US Companies operate in the best global environment to develop and sell high-technology products including cryptography. A US software development company can operate without any restriction on use of cryptography. US companies have unregulated access to a market of 260 million people who are the most advanced and wealthy consumers in the world. Contrast this with the situation of non-US developers who cannot access the security building blocks provided in operating systems. For instance, Baltimore Technologies cannot utilise the cryptographic subsystem offered in Microsoft Windows, the most popular operating system in the world.

Non-US companies have always been at a distinct disadvantage to their US counterparts, and have only succeeded by building better products.

4. Operating in the international market, Baltimore deals with an array of cryptographic regulations that require us to modify our products. We, as well as being developers of cryptographic systems, support competitive cryptographic systems from many other vendors.

5. Baltimore will welcome the global availability of strong-crypto versions of popular software such as browsers, email programs etc. The widespread availability of these products will encourage secure e-commerce and will enable Baltimore and other American and non-American companies to expand their business of providing security systems based around these software systems.

6. In our experience, export licenses are generally available to US companies for a great number of sales that Baltimore bids for throughout the world. Additionally, many US companies have bought foreign companies or establish non-American corporations to enable them to sell to a wider market. American companies are a formidable force in the global security marketplace.

RECOMMENDATIONS

1. The SAFE Act export provisions will let the "genie out of the bottle" in an inconsistent manner to that of other countries. An international approach to addressing the regulation of cryptography already exists in the form of the Wassenaar Arrangement.

Baltimore Technologies suggests that the issue of cryptographic export regulations be addressed on an international basis rather than in isolation. This is not a matter of the USA versus Rest-of-the-World . The twin concerns of the government and citizens of the United States are not dissimilar to those in other countries. US-based security companies have by-and-large similar experiences to that of non US-based companies.

2. Baltimore Technologies suggests that the differences in regulations between general products that include cryptography (e.g. Browsers) and pure cryptographic products are maintained.

3. As the leading nation in world commerce, the United States of America has an opportunity to create a global framework for e-commerce that incorporates the appropriate encryption policy.

Mr. TAUZIN. Thank you Mr. Holahan.

Now, Mr. David Dawson, chairman of and CEO of V-One Corporation of Germantown, Maryland. Mr. Dawson.

STATEMENT OF DAVID D. DAWSON, CHAIRMAN AND CEO, V-ONE CORPORATION

Mr. DAWSON. Thank you, Mr. Chairman. It is a pleasure to be with you today. V-One is a public company that has been providing network security solutions for over 7 years, which sort of makes us an old timer in this space.

Although we got our start providing security solutions to agencies of the Federal Government, Department of Defense, and so forth, today our commercial business outstrips our government business by two to one.

Our products are used by some of the world's largest companies, largest global corporations, so we have had exposure to both the public and private sector perspectives on this issues. We support the efforts of this committee to make electronic commerce viable and U.S.-developed encryption products competitive.

We agree that such commerce demands strong encryption capabilities. We also believe that H.R. 850's goals can be achieved through current regulations on the export of strong encryption in a matter that satisfies law enforcement, the courts, and the concerns of the private sector.

The issue is how to balance the interests of law enforcement while providing protection under the first and fourth amendments in an approach that is commercially viable.

Implementation of a mechanism for recovering encryption keys does not need to compromise these protections. We have seen techniques attempted and failed because they create undue administrative burdens and security risks that are clearly unacceptable to the private sector, such as third party or key escrow approaches or because they create back door access to plain text data.

Just because these attempts failed does not mean that the interests of all parties cannot be served by other solutions. V-One has developed a technique for recovering encryption keys that leaves the control of the keys with the company while providing limited conventional mechanisms for law enforcement to recover those keys.

This method, called "Trusted First Party," was recently approved by the Department of Commerce and is shipping today. If law enforcement wanted to obtain a document from your organization's file or safe, they would first have to convince a court that they had probable cause to believe that the document was being used in the commission of a crime.

If they were successful in convincing the court, the court could issue an order to have the organization turn over those documents to the appropriate law enforcement agent. We have lived by these laws and protections from excessive force and illegal search and seizure for some time and it would seem that they have served us well.

In crafting the requirements for industry to manage encryption, we believe that the Department of Commerce has merely attempted to apply current laws and protections for recovering documents to recorded secure electronic commerce.

Properly implemented key recovery simply extends current laws to the encrypted electronic world. Key recovery, when under the complete control of the corporate entity, is not in and of itself a security boon or bane.

In the realm of data communications, we would concur that it serves no useful purpose to the company. What the Trusted First Party approach does do is to provide key recovery that satisfies the concerns of law enforcement in a way that upholds the private sector's privacy and security.

Recently the U.S. Court of Appeals for the 9th Circuit in Berstein v. USDOJ determined that the requirements on Mr. Berstein to obtain export approval for his academic research constituted prior restraint of his freedom of speech. V-One has eliminated need for entities using the Trusted First Party technique to obtain prior approval from the Department of Commerce.

Because of this approach's approval by the Department of Commerce, individual case-by-case export approval is not necessary, thus eliminating the prior restraint issues raised by the 9th circuit.

In conclusion, our Trusted First Party solution works within current U.S. encryption law and satisfies, first, the courts by eliminating the need for government case-by-case export approval, thus avoiding the prior restraint of freedom of speech issues cited in the 9th circuit court.

Second, law enforcement, by providing a reliable mechanism for recovering individual session keys with a valid court order giving them the same ability they have today with nonelectronic communications.

And third, the private sector by allowing them to keep control of their own session encryption keys in a way that poses no additional security risks and by allowing them to use strong U.S. encryption technology today. This means that under the current law, any customer in a nonembargoed country can use any strength encryption to protect any application without a case-by-case U.S. Government approval.

And Trusted First Party has proven that this can be done today with virtually no additional finance or resource requirements on the customer's part. Therefore, we believe that current U.S. law relating to encryption exports can meet the interests of the private sector, law enforcement, and the courts.

The V-One Trusted First Party technique is a patent pending solution which requires significant expenditure and development on the part of V-One. In order to accelerate the acceptance of U.S.-developed strong encryption solutions without compromising the needs of law enforcement, we are willing to share this technology with other U.S. companies.

We appreciate the opportunity to be a constructive part of this debate on these important issues facing this committee and our country. Thank you for your time and attention.

[The prepared statement of David D. Dawson follows:]

PREPARED STATEMENT OF DAVID D. DAWSON, CHAIRMAN AND CEO, V-ONE CORPORATION

V-ONE Corporation supports the efforts of H.R. 850 to make electronic commerce viable and U.S. developed encryption products competitive. We agree that such commerce demands strong encryption capabilities. We also believe that H.R. 850's goals can be achieved through current regulations on the export of strong encryption in a manner that satisfies law enforcement, the courts and the concerns of the private sector.

The issue is how to balance the interests of law enforcement while providing protection under the 1st and 4th Amendments in an approach that is commercially viable. Implementation of a mechanism for recovering encryption keys does not need to compromise those rights.

We have seen techniques attempted and failed because they create undue administrative burdens and security risks that are clearly unacceptable to the private sector—such as third party or key escrow approaches—or because they create "back-

door" access to plaintext data. Just because these attempts failed does not mean that the interests of all parties cannot be served by other solutions.

V-ONE has developed a technique for recovering encryption keys that leaves control the keys with the company while providing limited conventional mechanisms for law enforcement to recover those keys. This method, called Trusted First Party, was recently approved by the Department of Commerce and is shipping today.

If law enforcement wanted to obtain a document from your organization's files (or your safe), they would first have to convince a court that they had probable cause to believe that the document was being used in the commission of a crime. If they were successful in convincing the court, the court could issue an order to have the organization turn over the documents to the appropriate law enforcement agent.

We have lived by these laws and protections from excessive force and illegal search and seizure for some time and it would seem that they have served us well. In crafting the requirements for industry to manage encryption, we believe that the Department of Commerce has merely attempted to apply the current laws and protections for recovering documents to recorded secure electronic communications

Properly implemented key recovery simply extends current laws to the encrypted electronic world. Key recovery—when under the complete control of a corporate entity—is not in and of itself a security boon or bane. In the realm of data communications, we would concur that it serves no useful purpose to the company. What the Trusted First Party approach does is to provide key recovery that satisfies the concerns of law enforcement in a way that upholds the private sector's privacy and security.

Recently, the U.S. Ninth Circuit Court of Appeals in Berstein vs. USDOJ determined that the requirement on Mr. Bernstein to obtain export approval for his academic research constituted a prior restraint of his freedom of speech. V-ONE has eliminated the need for entities using the Trusted First Party technique to obtain the prior approval from the Department of Commerce. Because of this approach's approval by the Department of Commerce, individual case-by-case export approval is not necessary, thus eliminating the prior restraint issues raised by the court.

In conclusion, our Trusted First Party solution works within current U.S. encryption export law and satisfies:

First, the courts by eliminating the need for government case-by-case export approval, thus avoiding the prior restraint of freedom of speech issues cited by the Ninth Circuit Court;

Second, law enforcement by providing a reliable mechanism for recovering individual session keys with a valid court order, giving them the same ability they have today with non-electronic communications; and,

Third, the private sector by allowing them to keep control of their own session encryption keys in a way that poses no additional security risks, and, by allowing them to use strong U.S. encryption technology *today*.

This means that under current law, any customer in any non-embargoed country can use any strength encryption to protect any application without case-by-case U.S. government approval. And, Trusted First Party has proven that this can be done today with virtually no additional financial or resource requirements on the customer's part. Therefore, we believe current U.S. law relating to encryption exports can meet the interests of the private sector, law enforcement, and the courts.

The V-ONE Trusted First Party technique is patent pending solution, which required a significant expenditure in development on the part of V-ONE. We are also keenly aware of the strong encryption export debate that has ensued. In order to accelerate the acceptance of U.S. developed strong encryption solutions without compromising the needs of law enforcement, we are willing to share this technology with other U.S. companies.

We appreciate the opportunity to be a constructive part of the debate on this important issue facing this committee and our country. Thank you for your time and attention.

Mr. TAUZIN. Thank you, Mr. Dawson.

The Chair recognizes himself for 5 minutes. Quickly, Mr. Schultz, what is your take on Mr. Dawson's solution?

Mr. SCHULTZ. I would like to see it.

Mr. TAUZIN. Grab a mike. I want to hear Mr. Arnold's take on it, too.

Mr. SCHULTZ. I would like to see it. The idea sounds good. I would like to see how it actually works. I would like to see how the protocols function; and, if it does work, it would seem to squarely

address, I believe, some of the problems that have been raised today.

Mr. TAUZIN. Mr. Arnold.

Mr. ARNOLD. I am not directly familiar with the solution itself or its implementation, so I would have to actually take a look at it and review it. It may hold a great deal of interest to us.

As it stands right now, I am struck by the fact that there is such wide availability through 128-bit cryptography out there that people who would be using this that would be investigated or, slightly nefarious, would probably not use key-recovery technology.

So any additional expense as far as managing the key-recovery technology or managing the resources and systems to do this would be borne by the people implementing it, basically legitimate businesses much like ourselves.

Mr. TAUZIN. Do me a favor. Take a look at and comment in writing to us on it. I would like to hear your comments on it, your take on it. Anyone else that would like to do that, I would appreciate that, just to see if we can get a balanced look at what is being proposed.

Mr. Reinsch, I want to turn to you and Ms. McNamara and Mr. Lee. One of the criticisms you make of the bill is that it would discourage the growth of voluntary systems. Mr. Lee pointed out in your testimony that the witness—that businesses already are key recovery to meet their own needs. I assume this is because it is in their interest to do so.

Why would a prohibition as contained in H.R. 850 on mandatory key recovery inhibit the growth of voluntary key-recovery systems or the use of Mr. Dawson's concept if businesses saw it in their interest to use that patented technology?

What is in the bill that would say that his solution couldn't work for people who wanted to use it and then voluntary key recovery is not now available and would continue to be available if businesses who want that type of a system? Any one of you.

Mr. LEE. Mr. Chairman, the provision that I was referring to is the provision in H.R. 850 that states that the government may not require or condition any approval on the requirement that the key be built in the hardware or software for any——

Mr. TAUZIN. Right. It is a provision that government cannot mandate key recovery. Why is that provision bad for businesses who want key recovery, might voluntarily want to adopt one of these things?

Mr. LEE. I think the point is that the government is encouraging businesses to take a look, as several of the panelists have testified here, at the requirement, the business requirement for key recovery.

One of the points that we would make is that in some cases the business requirement, that is the requirement of things that you have to do to make a profit and sell your product and be out there in the marketplace, includes complying with government requirements, regulations, and oversight.

In some of those cases it may be necessary to meet that business requirement for private companies to take a look at various systems that will enable them to guarantee them that they have access to plain text when they need it for a business purpose.

Mr. TAUZIN. You are saying the capacity of the government to mandate it serves as an encouragement of citizens to look at it. But we know from your testimony that citizens are not looking at it. Businesses are now developing it. What is wrong with that?

Mr. LEE. Mr. Chairman, it wasn't my testimony that the government seeks to mandate key recovery. Independent of key-recovery technology—the government has requirements that businesses make available certain records for governments, for agencies to perform their regulatory functions.

To meet those requirements, industry may need to take a look at various systems that guarantee that they can make plain text available. That was the point that I was trying to make.

Mr. TAUZIN. I need to move on, but I am going to ask you to please, any one of you, submit to me in writing a clear explanation of why you think a prohibition against mandatory key recovery in the bill operates to discourage voluntary key recovery for those businesses who like it, who want to use it. I missed that very badly. I don't understand the argument.

Quickly, I want to hear something more importantly from you, Ms. McNamara and Mr. Reinsch. Mr. Schultz and Mr. Arnold made a very compelling case that the national security interest of this country are threatened today, even our Gulf War operations were threatened because of the lack of highly capable encryption technologies being out there, and that absent policy to encourage the development of extremely capable encryption technologies, that national security is threatened.

You make the argument that the export and development of these encryption technologies itself threatens national security. We are getting it from both sides here. And the national security argument is very compelling to us in the Congress, as you might know, particularly on the day that the Cox Committee report is being released.

But we are hearing it from both sides. We are being told don't let this encryption stuff go forward because it will threaten national security. We are hearing national security is already threatened because of the fact—as well as business security and privacy and confidentiality all of the other things you are talking about, Mr. Arnold—are threatened because of the lack of a good strong encryption policy. Which is it? Ms. McNamara?

Ms. MCNAMARA. Mr. Chairman, first let me comment on our concerns about the prohibition of key recovery.

Mr. TAUZIN. Please do so.

Ms. MCNAMARA. As we read the language, it would prohibit the U.S. Government from also specifying that key recovery was the choice that they wanted to make.

Mr. TAUZIN. You mean in terms of its own procurements?

Ms. MCNAMARA. In terms of the U.S. Government's own way of dealing with U.S. Government communications. Correct. As currently written, it would prevent the U.S. Government from specifying that key recovery was an element of choice for them.

Mr. TAUZIN. But your concern is that the bill would prevent the government in its procurement policies from choosing a key recovery system?

Ms. MCNAMARA. Yes. In fact, the Department of Defense a year and a half ago—Bill, help me—specified that they would only use by date certain products that were key recoverable.

Mr. TAUZIN. Your concern is this bill would prevent that?

Ms. MCNAMARA. That is absolutely correct. That is our interpretation. And the government may choose to use that as a means of recovering data that they require.

Mr. TAUZIN. That is a separate argument from saying that others would not choose voluntary key-recovery systems.

Ms. MCNAMARA. And I am addressing our concern as the agency of government that is responsible for providing security for U.S. Government sensitive communications.

Mr. TAUZIN. I understand that concern. That one makes sense. The other doesn't and that is where I am lost.

Ms. MCNAMARA. I wanted to address that from our point of view. Regarding Dr. Schultz's remarks, I would say that he reinforced my statement that while encryption is available, it is not being widely used.

During the Desert Storm/Desert Shield arena, we have records where we did have strong encryption products available for use by U.S. Government forces, U.S. military forces involved in Desert Storm, Desert Shield; and we know that they weren't being used. People don't use it if they have to elect to use it.

Mr. TAUZIN. Let me touch on that quickly. Mr. Reinsch, you are saying you are amending government policy by granting encryption products at 128 bits or higher on request under waivers and certain circumstances. Mr. Gillespie points out in 47 seconds you can down load 128 bit encryption software if you want to use it.

But if I am a bad guy and I want to use it. I can get it off the Internet in 47 seconds. What purpose does your policy serve in hamstringing or handicapping the sale or the use of encryption products and export faith by America when the bad guys can already get it in 47 seconds.

Mr. REINSCH. I think there are several answers to that, Mr. Chairman. First of all, I think the downloading is, from our point of view, a question of confidence. If you have confidence in what you download from the Internet without necessarily knowing its providence, then fine, you can use that encryption.

Mr. TAUZIN. You are saying that it is not a good system?

Mr. REINSCH. I am saying that you don't know that when you download it. Sometimes it is and sometimes it isn't. And it is not easy for the customer, in particular, to know with certainty what he is getting when he obtains encryption through that device.

Now, if you want to do that, that is fine. We have never claimed in any of our statements that the effect of our policy is perfect in the sense that it prevents terrorists, drug dealers, or whoever from obtaining robust encryption and utilizing it if that is what they choose to do.

We are trying to influence market developments at the margin. We are not attempting to deal, because we cannot for the reasons that you said, with every possible contingency.

Mr. TAUZIN. My time is up, but I want you to comment quickly on one of Mr. Hornstein's arguments that the regulations of our government, particularly in incapacitating his executives from com-

municating with companies overseas in these contracts to which he is saying he is handicapped, is harming U.S. companies' abilities to win those contracts. Your comments, quick.

Mr. REINSCH. Well, Mr. Hornstein and I probably need to have a private conversation about the particular cases. Let me just say with respect to the first one, he has correctly stated the status of the item that he wants to export. He came in for an advisory opinion, and we told him what he said.

As far as we know they have not actually applied for a license to export that item, and I don't think that it is fair to assume that such an application would be denied if he were to submit one. We try to work with companies to address the kinds of problems that he is reflecting here, and I am not sure that we are entirely responsive in his case.

Mr. TAUZIN. I think what he said was in the meantime his people can't communicate without violating your regulations. Is that true, Mr. Hornstein?

Mr. HORNSTEIN. Yes.

Mr. TAUZIN. Is that a real problem?

Mr. REINSCH. What we said in the first case was, in order to provide technical assistance to his people, in order to provide that communication, his people would need an export license. He is correct about this.

If he would come in and ask us for an export license, which he has not done, and then we were to deny it, he would have a better point.

Mr. TAUZIN. I want to understand how that works a little bit better, and maybe we will get to that later. The gentleman from Massachusetts.

Mr. MARKEY. Thank you. Mr. Holahan, thank you so much for coming from Dublin. It is no wonder you have such a keen interest in encryption issues, because without question the first commercially available encryption technology did come from Ireland. It was James Joyce's "Ulysses."

It was the greatest book every written, although very few people have read it; and those that have concluded, finished reading, the book have no idea what it was that they read.

Mr. HOLAHAN. You do have to decrypt it. Ten pints of Guinness will decrypt it.

Mr. MARKEY. The Irish would be good at this. So my question will be this. For instance, as I said earlier that security and privacy are the flip sides of the same coin. Obviously, Americans want both. The people here can help us maybe to square this all up today.

So when I encrypt my cell phones by subscribing to a digital technology so that the contents of my conversation is pure and private, at the same time there is a company who knows who I called, when I called, from what location I called; and that is very highly valuable information. It is both.

So the company has my valuable information now. That is why we have laws and rules over how telephone companies can disclose our phone calls. They just can't hand this stuff out to people. It is very private, who we call, when we call, from where we call.

Similarly, on the Internet making my on-line purchases more secure, my on-line stock trading encrypted and secure and encrypting the contents of e-mails and computer files helps to foster electronic commerce and promote privacy. And that is good. I don't want people to be able to crack in.

Yet, regardless of whether I send an e-mail or consummate an on-line transaction, simply knowing which on-line sites I visit, when I visit those sites, how long I linger on certain pages is also highly valuable and may be highly personal information.

Shouldn't companies have an obligation as telephone companies do today to allow me to protect the confidentiality of what places and sites I call upon with my computer?

Mr. Schultz, do you believe that I should have a legal right to block a company from using that information for any other purpose other than that which I originally attempted?

Mr. SCHULTZ. I am hesitant to plunge into that arena from the standpoint that the behavior is so firmly established as far as being able to tell who hit your web site, who hit your file transfer site, and things like that. To reverse that around is a radical departure from computing norms.

Mr. MARKEY. So your concern is that the government could crack in, but you are not concerned that others could crack in?

Mr. SCHULTZ. In terms of being able to grab the information and thus reveal information about individuals, right. And if I actually hit Playboy.com or some other site and there is some concern now because they are the priest of a church or something——

Mr. MARKEY. That is very scary.

Mr. SCHULTZ. But it is well-established behavior.

Mr. MARKEY. I know, but we have to reverse that. You are here representing ordinary people. You are saying that they should be given security. They should be given privacy from the government.

And yet when I raise the question of companies compromising or individuals compromising my privacy, my electronic commerce, you say it is gone, it is lost. Whereas we could pass a law here to get protection for that as well. You don't you think we should?

Mr. SCHULTZ. I don't think that you should.

Mr. MARKEY. You think we should.

Mr. SCHULTZ. I don't think that you should.

Mr. MARKEY. Why not?

Mr. SCHULTZ. The reason is that when you play in a public playground, which the Internet and the many other public networks are——

Mr. MARKEY. Do you consider the telephone network a public playground?

Mr. SCHULTZ. Less so.

Mr. MARKEY. Do you think Americans consider their on-line commerce, their on-line trading, their children heading out to web sites to be in any less need of privacy than the telephone calls their children make or their families make? You think Americans believe that?

Mr. SCHULTZ. I believe that many Americans believe that it is a different ball game playing out.

Mr. MARKEY. You couldn't be more wrong on that. People don't want as they move over from the telephone to the computer mak-

ing the same transactions to have that stuff out into the public domain so that any company can compromise it.

My problem with you, Dr. Schultz, is that you can't square up this policy. You can't sit here and testify about how concerned that we should be that the government could crack into the privacy of Americans.

By the way, I would trust them more in many instances than I would trust many of the companies that you are representing in terms of preserving and protecting the privacy, the security, the integrity of this information.

I see you here representing corporations, but I don't see you here representing the American people today. I support your policy on encryption. I think that I have a right to that encryption, sir.

But I think I have a right to be protected against your company, too, reusing my information. Is there anyone here, any company here, that believes that we should be able to pass a law to protect against the reuse of the information which is gathered by your companies for purposes other than that which the individual, the family intended? Will anyone here testify to that? Good. Mr. Arnold.

Mr. ARNOLD. Let me jump into this fray if I may, Mr. Markey. I think there is several issues on the table with regards to privacy and subsequent use of the information both by the company and then unintended use by someone who either penetrates the system.

One of the major concerns that I think that we have is the longevity that the data sits in various data bases and the length of time it may be accessed. I think that is one of the major arguments for the use of hardened encryption to these systems. It is also to keep private information on individuals, on customers, on consumers from being seen by people who have absolutely no need to see it within the organization and outside the organization.

Mr. MARKEY. My question is should you give the individual a right by law to deny the reuse of that information? Should it remain in the company's purview as to when it is used and whether it is sold to other people? How do you believe? What do you think?

Mr. ARNOLD. I can answer. Personally, I believe that it should be up to the person to deny subsequent use.

Mr. MARKEY. Thank you. Does anyone else on the panel agree with Mr. Arnold? No one else? That is a problem for me. Essentially, the policy is burglary is okay as long as the company leaves a note saying, well, we took this information, and we are giving you notice that we are selling it all.

But you don't have any legal right to block us from reselling any of this information. We can burgle all of your private information. All of the information we want to keep governments from gaining access to, we can burgle and sell for profit for our company.

I have a problem. Mr. Arnold, at least you believe that the individual has some right to protection from a company compromising that which we don't want the government to compromise.

Mr. ARNOLD. I would add also that the major thing that a consumer looks for is the fact that they don't want somebody masquerading as them on the Internet.

Mr. MARKEY. Exactly. Mr. Hornstein.

Mr. HORNSTEIN. I am just confused at the comparison. I understand that we are debating here about encryption and the exports internationally. But your example, which is just with the Internet, how is that different from Visa and the paper process of obtaining information or somebody sending a letter in the mail with an address or return address on the corner and then people processing that in a manual system. I don't understand how those two are brought together in the context of this discussion.

Mr. MARKEY. Because you are telling us that everything is going digital, everything is going on line, all commerce is going on line and as a result everything is much more vulnerable.

My question to you is as we move through this era and you warn us what the government can do as we move into this era, should we also be apprehensive of what it means for individual privacy, for children's privacy in our country?

In other words, the point that I am making again, it is the other side of the same coin, privacy and security, the government and the private sector. And the question is whether or not the industry can have it both ways.

They can say it is a serious issue when the government is going to be able to intrude, but it is not a serious issue if they are going to compromise the very same. I don't think that you can have it both ways. I think you have got to be on one side of the issue or the other. I don't think that you can have it both ways. And I genuinely—I will be glad to yield.

Mr. STEARNS. This might be supporting what you are saying. If I bought products from L.L. Bean, is L.L. Bean able to make public my selections; or, for example, can the telephone company make public all of my calls? No. I think that is the case that you are making.

Mr. MARKEY. The telephone cannot.

Mr. STEARNS. Can L.L. Bean?

Mr. MARKEY. Yes.

Mr. STEARNS. So then what you have to decide is differentiate between a company like L.L. Bean can make it public, but if a phone company can't, the phone company is sort of quasi-regulated. We have to be consistent.

Mr. MARKEY. If I may——

Mr. STEARNS. Can't MasterCharge and VISA disclose too?

Mr. MARKEY. Yes, quite briefly, as all of the health care information goes from being in a file where you walk in and the doctor and the nurse have your file and have had it and your children's files since the day they were born.

We are moving into an era where the HMOs and the larger health care consortiums are now taking all of those files out of their hands, computerizing it, finding out who has all of these various ailments and whatever; and now they can market it to other companies who they would never market it to.

So what happens is that as we move from this era of where we had privacy keepers, we now have the capacity where the data mining keepers are able to take it and create information, DNA about our families. That's what all of these industries are all about.

They don't want the government to be able to crack in for their security. My question is should, as the new era unfolds, should we

put a set of protection upon the books because it has never been possible before. Yes, in limited cases, L.L. Bean or whatever, but now we are talking about all of your financial records and all of your health care records for you and your family.

I think that we should discuss it. I don't think that as yet the industry has squared up their concern about privacy and security with the American individuals that also need to be protected. You haven't done it.

Mr. TAUZIN. The gentleman's time has expired. Let me, for the purposes of the committee, point out that the weekend retreat we have scheduled in July we will be focused on this and very similar issues involving the movement to digital in the Internet.

I would again encourage you all to make sure that you put aside time for that weekend, 14, 16, 17, sometime around then to be with us for that retreat. CATO just completed a privacy session on many of these issues that Mr. Markey has raised. We are going to be faced with them very shortly as the Internet becomes a place for telephony.

You know, the AT&T cable merger is designed specifically in that area, to define a new way of us reaching each other over the Internet with pictures and audio services. That Internet telephony is not covered by the prohibition that prevents the telephone companies from marketing that information. That and similar issues will be raised at that retreat.

I use the occasion of Mr. Markey's comments and questions to remind you these issues are going to be before us rapidly. Make sure that you make time to be with us. We are going to have some healthy discussions about them at our retreat. The Chair now recognizes the gentleman from Ohio, the Vice Chairman, Mr. Oxley.

Mr. OXLEY. Thank you, Mr. Chairman. Mr. Dawson had a response, I think, to Mr. Markey's question.

Mr. DAWSON. I was just going to add to what you said. Your idea of the company being able to use that information, I think if someone visits my web site, the fact that they visited my web site as V-One is information that the company has a right to, not a right to necessarily to share with other entities. I think that's your point.

I appreciate web sites, when I go to a web site that if I put some information about myself and it says check this box, do you care if we provide this information to others. I think you are correct, that that should be regulated some way to prevent massive invasion of privacy. I think that is a bit different issue than the encryption export issue.

Mr. TAUZIN. Would the gentleman yield a second? I will give him—just for 5 minutes. I want to point out that there is in the marketplace today, however, just as you have developed a marketplace solution for key recovery, there are marketplace software solutions being developed.

Novell, I know, has one that will allow you to control completely your entry into cyberspace, all of your medical, financial, all of your records, all of your information in a way that you define your own identity in cyberspace.

There are several other companies. I don't want to cite just Novell. There are quite a number of others. We are going to get a look at all of those at the retreat again. We have the option of ei-

ther legislating or facilitating the development in the private sector, some of these technologies. The gentleman is now recognized.

Mr. OXLEY. Thank you, Mr. Chairman. Let me just say we discussed this last time. Had we had a situation like the World Trade Center bombing, the Oklahoma City disaster, the Littleton rampage, and had it been revealed later that the perpetrators had planned all of this using encrypted communications, what do you think the public outcry would have been had this legislation passed?

My guess is that the public outcry would be strong against your department, Mr. Lee, perhaps against yours, Ms. McNamara, and perhaps all of us who saw fit to not provide the kind of protection for the public that is our solemn responsibility.

Does anybody have a different feeling about that? If indeed that is the case, then doesn't Mr. Dawson's proposal start to point us in the right direction as to how we can solve the problems of technology with technology?

I was going to ask Mr. Reinsch, because of the Commerce Department's biennial review, whether, as I view it, this legislation is unnecessary. Let me ask Ms. McNamara, based on your review, is this legislation necessary and if so, why?

Ms. MCNAMARA. Thank you very much for that question. On behalf of the administration, I would say that the administration does not believe that export control legislation with regard to encryption is either necessary or desirable.

We believe that relaxation as we demonstrated last October and as the Wassenaar Arrangement signaled in December that we can relax much more quickly under the current regulatory regime that we have.

Were legislation to be passed each time we wanted to relax, we would have to come back to Capitol Hill and say, mother may I, or father may I. In this particular case under the regulatory process, we have relaxed to a substantial part of the world's economy recognizing that there were segments of the world's economy that needed to be afforded protection and that was with consultation with industry.

Now we excluded some segments of the world's economy from blanket release of encryption or relaxation of encryption and encryption products. But we still maintain on a case-by-case review the possibility of individual licenses being issued for the export of strong encryption and encryption technology to other segments that are not covered by the broad relief.

Those individual licenses are being granted today. They have been granted this year. They have been granted because, through the technical review afforded under the current regulatory regime, we have a technical review of products so that we understand how they are going to be used, by whom they are going to be used, and what purpose they are going to be used.

Mr. OXLEY. Mr. Lee, do you agree with that?

Mr. LEE. Mr. Oxley, the Department of Justice fully supports the administration's view that H.R. 850 is not necessary. Our primary interest and mission, of course, is domestic, but we fully support the needs of the national security community, and we are, of

course, a customer or partner with the national security community.

We believe that the existing regulatory regime in which the Department of Justice and FBI participate is a flexible one that takes into account all of the needs that have to be balanced here, the needs of the commercial sector, law enforcement, national security, and the needs of individual users.

Mr. OXLEY. Would the President veto this legislation, Mr. Lee?

Mr. LEE. I don't have a view or information about that.

Mr. OXLEY. Ms. McNamara?

Ms. MCNAMARA. I don't have a view, sir.

Mr. OXLEY. I was hoping to ask Mr. Reinsch that, and he had to leave. But I would be interested in what the President's senior advisors may recommend.

Mr. TAUZIN. If the gentleman would submit a written question, he has agreed to answer in writing any questions we give him.

Mr. OXLEY. That would be fine. I would appreciate the opportunity to do so.

Mr. HORNSTEIN. Can I make one comment on the licensing program we are talking about here? We have done many, many licenses for filing with the Commerce Department, and we find the process is arbitrary. We have identical consumers, foreign, in different countries who for whatever reason when we actually did them, we filed for the export license.

One was denied and one was approved. There is no guarantee when you are out there trying to sell a product to a legitimate global 1,000 consumers why in one situation they would be approved and one situation they would be denied.

Mr. OXLEY. Mr. Hornstein, you mentioned the product from Israel?

Mr. HORNSTEIN. The double check point.

Mr. OXLEY. That you are competing against? Do the Israelis have some form of key recovery?

Mr. HORNSTEIN. Do the Israelis have key recovery? No. Let me go through key recovery, if I could take 1 minute with you. There is a difference between government key recovery and a corporate key recovery. We have had the other panelists down there explaining they had a key recovery product. We have had key recovery products for years.

Mr. OXLEY. The Israelis have no key recovery at all?

Mr. HORNSTEIN. I don't know the answer to that. It depends upon the consumers, if they want them. We have a corporate key recovery product.

What it does is if you have an individual who is communicating within a corporation and if they get hit by a bus and they cannot go back and find out what was the communications they have had this very day, the CIO or the MIS director in that company has a corporate key which will allow the person to open up all of the communications within that company.

We have had that as an offering for many years. That is something that is built in as a customer offering. But if you are talking about whether an international company will actually implement that and make a requirement for them to make a corporate key recovery, that is something on an individual basis.

But there is an ability for a centralized location in many of our products to have a key recovery as a—after the corporation, but it is not held by a trust or third party and it is not held by a government entity. We have found in experiences that nobody will buy that internationally.

Mr. OXLEY. Ms. McNamara?

Ms. MCNAMARA. Mr. Oxley, first let me say that I don't know whether Israel has key recovery or not, but I do know they have an export control regime. The Israeli government has in place a process to review all products for export. We know that because we have had those conversations. That is the first part.

The second part is we will always have different answers through the licensing regime because end use and end users are what we use to justify the national—to understand and vote on from a national security perspective, whether or not somebody should export to a certain end user or particular location. That is a matter of U.S. Government policy as well.

There are a series of pariah nations that fall into that category, and the U.S. Government uses that for the enforcement of our own foreign policy. With regard to the number of denials, this year, 1999, one, precisely one, license has been denied.

Mr. OXLEY. Thank you. Mr. Schultz?

Mr. SCHULTZ. I would just like to add that I think the problem is not being adequately scoped. The problem is we are fighting battles over encryption which now is really considered fairly weak by international standards, but we are still drawing the line there.

We need to move our sights up into even stronger encryption and let go the little battles over the weaker encryption. I will tell you right now most 128-bit encryption is weak encryption now.

Second of all, real important, and I will yield, but it is important to understand that crypto doesn't work unless you establish a culture of cryptography within your organization, within your institution, within your industry. That is the problem with this license-by-license application problem.

It does not let encryption enfuse itself in the culture. It now becomes an "iffy" question for corporations, for industry, whether or not they are going to use it. I therefore strongly do not favor that.

Mr. OXLEY. Mr. Dawson and then we will——

Mr. TAUZIN. Yes.

Mr. DAWSON. I think Dr. Schultz makes a good point about establishing a culture of crypto and people won't use it if it is difficult to use. I want to clarify one thing. The key recovery mechanism that we are talking about, we have included free of charge to our customers.

So No. 1, it doesn't create that kind of a burden. And from an administrative burden, I think it is reasonable if a company has a security administrator for the corporation, which most do, that person is also the key recovery agent, should a court order appear on the doorstep. Beyond that, there is very little required. I just wanted to clarify that, that this isn't an onerous hard-to-use burdensome-type of approach.

Mr. TAUZIN. Thank you, Mr. Dawson. The Chair is going to have to excuse Ms. McNamara on her time request as well. Before you leave, Ms. McNamara, let me ask you to respond in writing. Our

language in the SAFE Act, H.R. 850, says that encryption products are allowed to be exported when they are generally available, I think is the term we use in the act in the world market.

If that is not a workable standard—and it may not be—we should hear from you on it. I would very much like to you hear from you if there is a better standard. If we are going to pass an act what should be in the act other than this generally available standard and whether you could suggest one, and would you be willing to suggest one. No need to respond now, but perhaps you could communicate this in writing.

Mr. LARGENT. Would the gentleman yield? If she is leaving, I just have a question I would like her to respond to.

Mr. TAUZIN. Let me do this. Let me ask each one of you to do that right now. Anna Eshoo is up next. Anna, if you have a question for Ms. McNamara, go ahead and ask it now, and we will get a response in writing.

Ms. ESHOO. Thank you, Mr. Chairman. Since you need to leave, I want to pursue what the chairman just brought up about standards and your concern that if the standard is not correct it opens the flood gate to exporting any and all encryption products.

My frustration on this issue since January 1993 is that the administration has really never come up with anything. The administration has shopped around different ideas and there have not been takers.

But the responsibility still lies with the administration and all of its agencies to come up with something and to work with the Congress. Now, the Congress has a bill on the table, a bipartisan bill that has, I think, today 253 cosponsors.

So I understand that the agencies have come to the Hill; they have literally scared the heck out of members that don't know very much about encryption, saying you are going to have blood on your hands if there is another World Trade Center bombing.

There isn't any Member of the Congress that doesn't want the security of our Nation protected, but we also want our economic security to continue to expand.

Ms. ESHOO. So I really urge the administration in every way, shape and form to come up with something. I think that you need to come back to this committee, as we do our consideration, to place before us language that would agree to allow the export of encryption products and to find what is currently available—what is out there in the business world that is currently available, you are rejecting today. So you are going to have to come up with something.

Another question that I want to ask you is, just over 2 weeks ago, the Ninth Circuit Appeals Court affirmed an earlier decision that in the name of national defense the U.S. Government should not restrict the very liberties it is supposed to be defending, which really exemplifies the judicial branch's understanding of the encryption debate. Would you comment on that?

Ms. MCNAMARA. I believe the chairman asked that question earlier, Congresswoman; and I believe Mr. Reinsch agreed to submit in writing an answer to that question, if I recall.

Ms. ESHOO. But do you have views on it?

Ms. MCNAMARA. The administration——

Ms. ESHOO. I can read the record. I am asking you.

Ms. MCNAMARA. I have my own personal views, and we are——

Ms. ESHOO. Not personal, public views on it.

Ms. MCNAMARA. We—we as part of the administration—are looking at that decision and deciding what our options are.

Mr. TAUZIN. Will the gentlelady yield?

Ms. ESHOO. Yes.

Mr. TAUZIN. Just to point out, then I will ask you to yield to gentleman from Oklahoma, too, that the Chair announced at the beginning of this session that we will be joining in a letter to the administration urging them not to appeal that decision, rather to work with us on appropriate legislation, and the gentlelady may have an interest in that.

Would the gentlelady now yield to the gentleman from Oklahoma?

Mr. LARGENT. Yes. I have just have a brief question, so you can respond in writing. I won't keep you any longer.

I found it interesting when you responded to Mr. Hornstein's comments about denying certain questions and your consideration is the end user. And I guess my question that I want to have you respond in writing is, what is the NSA's view as an end user of the People's Republic of China and the Red Army in terms of transferring military, missile, computer technologies?

So if you could respond to that question, I would appreciate it, too. You don't need to respond now.

Ms. MCNAMARA. Let me just tell you, I am pleased with the question. I was expecting a question related to China particularly, because of the Cox Commission report being released today; and as part of my homework assignment, I read the Chinese regulations with regard to the use of computers, Internet, and encryption and what the impact of that is on—both in terms of both import and exports. So I will be happy to answer that question, Congressman.

Mr. TAUZIN. The gentlelady's time is extended.

Ms. ESHOO. Thank you, Mr. Chairman.

Thank you, Mr. Arnold, for coming across the country. Mr. Arnold, I should state for the record, is a constituent.

I am sorry that I wasn't here for everyone's testimony, but I want to thank you for being here today and working with us on this. You can tell from my statement to Ms. McNamara that this is an area, both in terms of encryption and export control, this is highly frustrating and an area where, in my service in the Congress, we have made very, very little progress on. So we have to try to keep pushing the edges of the envelope out.

For Mr. Lee, currently, the 128-bit encryption is generally available, we know, from many domestic companies for sale within our own country and from a number of companies for sale abroad. Does the Department of Justice oppose raising the allowable exportable limit to 128 bits; and, if so, why?

Mr. LEE. Congresswoman, as you are aware, the administration in the recent export regulation updates permitted the export of 128-bit encryption to a number of very important sectors, and those include U.S. companies for their internal use, and they include the use of on-line merchants for use in securing transactions with their customers abroad and other sectors. So the Department of Justice

fully supports the spread of 128-bit encryption when we believe it is consistent with the public safety needs of our Nation.

We would be pleased to participate, and we are in ongoing regulatory reviews that look at to what extent encryption can be made available, very strong encryption to other users, other sectors abroad, consistent with public safety and law enforcement needs.

Ms. ESHOO. How do you define public safety in this area, just briefly?

Mr. LEE. We define——

Ms. ESHOO. You are responding to it in your response to me.

Mr. LEE. Yes, ma'am. We use public safety to refer to our mission and our responsibilities to enforce the laws of the United States. That accounts for any number of statutes. It is a very broad reach.

Ms. ESHOO. Very broad. It is just—it really is quite instructive to me how the element of fear, which is one of the most powerful emotions on the scale for human beings that has been used very effectively in this whole debate, and I don't know how we can, Mr. Chairman, move that one aside, to set it aside and have the discussion about the technologies.

My sense is that both within security agencies, the law enforcement agencies, that they are having an enormously difficult time keeping up with the technologies and being able to handle the codes and break them in the work that they do, very legitimately, in law enforcement. And, as a result of that, the national emergency brake has been pulled up and said, no, no, no, wait a minute, we have to slow this down, we have to keep a lid on it, because we can't keep up with you.

I can't help but sense, after all of the hearings I have been in, and I have gone from one committee to the other to hear the presentations that both national security and law enforcement have made, and I can't help but come to that conclusion.

Did you have a comment that you wanted to make?

Mr. GILLESPIE. I did, Congresswoman. Thank you very much. I think you raise a very valid point.

And we saw here today even and we have seen it in the past, is that administration has shifted the nuance of their argument quite a bit. You know, they used to come up here and say, we have to stop this. We have to have these export restrictions. Because, if we don't, this strong encryption is going to become very widely available. And, of course, they can't counter the fact that there are now over 650 products on the market from over 29 different countries.

And so, if you noticed today, the nature of the arrangement changed to be, well, yes, it is widely available, but nobody is using it yet, and we ought to stop them before they start using it. Of course, it is widely available because of the consumer command.

I think in terms of the point that you made about the national security aspect, there is some new thinking going in the national security community. I would commend to the committee's attention a report released by the Center for Strategic International Studies. The report was chaired by Judge William Webster, who is a former director of the FBI and the CIA, and a former U.S. circuit judge. That report is called Cybercrime, Cyberterrorism, Cyberwarfare, Averting Electronic Waterloo.

And if I may just read one quote from the report released by Judge Webster, he notes here that it 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 strategic information warfare needs of the 21st century. Continued reliance on limited availability of strong encryption within the development of alternative sources and means will seriously harm law enforcement and national security.

That is not industry saying that.

If I may make one other point, Congresswoman and Mr. Chairman, there has been a lot of discussion today about the Cox report. And if the committee is amenable, perhaps Congressman Cox's own OpEd in the San Jose Mercury News from March 27th in which he says some have inferred from his report this should mean clamping down on commercial exports. To the contrary, the committee found—his committee found the current export licensing processes riddled with errors and plagued with 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. He says, I disagree with the Clinton-Gore administration that the current prohibition on American businesses export encryption software is necessary for our national security.

So I think, in terms of the implications of the Cox report, perhaps we ought to have the chairman's words speak for—rather than some others representing and inferring from it.

Ms. ESHOO. Mr. Chairman, just—thank you for that, Mr. Gillespie.

I just have a quick question to Mr. Arnold. While I have this going through my mind, I think that we should have a review of that report presented by someone that helped to write it when we have our retreat, because I think it fits into that.

For Mr. Arnold, you covered briefly in your opening remarks, but I would like you to expand a little bit on what effect you see the administration's current encryption policy having on emerging E-commerce? It is a huge area in our country. It is a great interest not only of the chairman of this full committee but all of its members. Maybe you can tell us what you have found with your international customers. Are they demanding stronger encryption products than you are currently allowed to offer? Just throwing you a softball ball, because I think I know the answer. I think it is important to have it in the record.

Mr. ARNOLD. I think they are demanding, there is no question about that. And, given the current policy, we had an encryption—we had a permit issued to us 2 years ago for a product that we had to the merchant sites to allow the merchants to communicate securely with us, and we made application of a new product going out.

The application went out in the January timeframe, and the product was launched in the March timeframe, and only as of late last week we were told we have another 60 days to wait before we are reviewed. We have not even seen an office action or even a question back to what we are doing.

And I think there is a great deal of confusion when we look at Internet commerce and electronic commerce here. Because looking at individual uses and what is the user who, you know, is getting it out there, there is hundreds of merchants out there, and what we are protecting is private information of the company, delivery information potentially that is going out there, that they are using to communicate with the delivery source.

We are protecting, of course, the financial information on the credit card; and we are protecting the information on the consumer themselves, is what is actually happening there.

But the individual end users are wide and varied. There are hundreds of them. And for the products that they themselves are selling, there is tons of those products as well that they are selling out there. So, you know, that has been probably one of the major issues for us going forward, is just trying to educate and to allow people to understand what this marketplace is that is expanding on the Internet.

On the other side of it, I would suggest to you that the criminal and nefarious acts that are going on, on average, run about 12 percent of the total transactions per day. And trying to gain some visibility within the law enforcement community over the past several years has been extremely hard to do and to educate on this.

And I really applaud the administration recently on setting up the Internet Fraud Council through the FBI. I think that is an absolutely excellent first start. I think the piracy work that the FBI is beginning to step in and do is absolutely excellent. But they are just barely touching the surface of what is actually going on out there.

Ms. ESHOO. Thank you.

Mr. TAUZIN. Thank the gentlelady.

I might out point out, before I yield to my friend from Illinois, that our sessions have indicated several things; and maybe you all can think about that in terms of responding for us.

One is that, FBI, the reason we put the language in the bill regarding the establishment of a lab at the FBI was the concerns we heard from the FBI. While they can use the NSA labs, they can't necessarily use the NSA personnel in a case to try to catch the criminal and can't necessarily use the people as witnesses to try the criminal because that would compromise NSA facilities and personnel. There is some real problems there that we are going to invite a lot of you to think about and help us resolve.

The gentleman from Illinois, Mr. Shimkus.

Mr. SHIMKUS. Thank you, Mr. Chairman.

As a cosponsor of this legislation, I found the debate and discussion very interesting. I also found it interesting of the continued comments about there is no need for this legislation. And I would submit, Mr. Chairman, that because of our movement on legislation last year that maybe the administration has, as I said, moved to at least relax some of their export controls. And whether you don't get the end result by passing laws, the movement of the legislative process does make some—you know, starts opening up the competitive market field. So the question what comes first, the chicken or the egg in this case, and I think our legislation which we tried to move last year.

Mr. Lee, in reference—since you are the only administration person left, I guess I have to direct this toward you. The administration's current policy doesn't require encryption product exported to certain market segments to be recoverable, that is, new relaxed plan. Doesn't this undermine your claim that all encryption products should be recoverable?

Mr. LEE. I think what I have testified both in this forum and other fora is that law enforcement has needs that, in order to continue to protect public safety, need to be met. There is a balance here. We participated in and fully supported the balance that was struck with the updates last fall.

We recognize, as with all encryption, as many of the members have stated, that there is an upside and a downside. It seems to us that the needs for strong encryption in those sectors, which we supported, really outweighed the possible harm to the public safety, but it would be remiss of me not to say on this record that there is a possibility that that strong encryption out there can be used for nefarious purposes by criminal elements.

So, again, there is a balance. We are trying to participate in that balance, but the ultimate goal is, when there is lawful authority for an interception or to seize stored data that happens to be encrypted, the ultimate goal would be that we able to obtain the plain text of that information.

Mr. SHIMKUS. When we relax export controls, you are, in essence, shut out of some communications, use in these market segments, am I correct?

Mr. LEE. When you say "you," are you directing that at me?

Mr. SHIMKUS. The administration, the Department of Commerce. When we decide, when we make a decision—I mean, it is really just follow-up to what you just said. We can't be—if we are going to allow and ease export controls, you can't assure me that that possibility now—there is a possibility out there that you can't have access to some information?

Mr. LEE. I think you have put your finger on the central dilemma with any effort to relax export controls. That is correct.

Mr. SHIMKUS. And let me move to Mr. Holahan.

I was interested in your statement, and I think we have this perception, you probably said it in your opening comments, but I would like you to elaborate. And I am a cosponsor of the legislation, and I like our high-tech industry. I want it to be competitive.

But just elaborate on, you say that Baltimore Technologies refutes suggestions often made that nonAmerican companies flourish solely because of the current export policy.

Mr. HOLAHAN. Yes.

Mr. SHIMKUS. If you mentioned it before, I apologize——

Mr. HOLAHAN. No problem. That was actually a comment taken from the testimony before the Committee on the Judiciary. That phrase was used, "flourish solely," because—just to give some examples, and this probably applies to Checkpoint software from Israel. We actually do sell our products inside the United States, and we were the first people to offer a job of cryptolography, not because we could do it, we just did it. And we sold it to, at the time, the leading security company, Security Dynamics; and they licensed it.

So we set inside the U.S., based on just our technical merits, not because we have got some advantage outside. So if it is a question of us not on a level playing field, why would we actually succeed in here?

We also—the major people that buy security, you know, the criminals don't come to us and buy security. Criminals will steal the security software if they want to. The people that buy security from us are people like banks, okay?

Banks—if a bank comes up with a requirement for security, they will go to a U.S. corporations, to Baltimore Technologies. They will go everywhere. And they can get an export license for the U.S., and we regularly compete against American corporations and win deals purely based on technical merits.

I would like to add that actual crypto is available everywhere, but the industry, you know—crypto is available everywhere, including the United States, but people are not even using it. The reason they are not using, because the software companies don't exist.

What we do is not just write crypto, we actually use crypto from the U.S., from the UK, from Canada, from France and Ireland. And what we do is build products on top of it to encourage people, as Dr. Schultz said, to actually use the crypto. Because crypto has been around for 25 years, but no one needed to use it. So it has been incorporated into the software products.

And that is—our job is not writing crypto. A very small percentage of our business is based on crypto, as is here is something that generates keys for you. The vast majority of our business is in the management systems which—actually, what we call cryptoagnostic. We don't care what crypto you use—U.S., recovered key crypto, IBM crypto, Intel crypto. We don't care what it is, because our value is in the management of crypto which is, in general, encouraging them to use, and that is why we succeed inside the U.S. So flourish solely, absolutely refute that, yes.

Mr. SHIMKUS. So you probably have multiple product lines then, in essence.

Mr. HOLAHAN. Yes.

Mr. SHIMKUS. And there is a separate one for U.S. import?

Mr. HOLAHAN. Unfortunately, yes.

Mr. SHIMKUS. Yes, sir.

Mr. GILLESPIE. Mr. Chairman, I was going to point out that the fact is perhaps Baltimore does not flourish solely because of the encryption laws. But there are a number of companies who aren't flourishing because of the encryption laws.

And, in fact, if you go on to the Siemens website, you will see where they market specifically directed at the export restrictions; and it says, here is where you can purchase the strong encryption products that American companies are not allowed to sell you. And that is the kind of marketing that is taking place across Europe.

I should also point out, because the Wassenaar Arrangement isn't brought up here, it was brought up by Mr. Holahan and others, the fact is that the Wassenaar Arrangement sets a floor, not a ceiling, in terms of crypto policy. And, frankly, our administration is below the floor that it set in the Wassenaar Arrangement, because Wassenaar allows for 64 bit, and we are still operating at 56

bit. So it would be nice if they would bring our policy up consistent with the floor at least in the Wassenaar.

Mr. SHIMKUS. And that is one of my questions I would have asked the Commerce guy. When do they perceive moving up to that level of 64?

Mr. HORNSTEIN. I don't know.

Mr. TAUZIN. A good question. Submit it in writing. We will do that for you.

Mr. GILLESPIE. If I might, Mr. Shimkus, in terms of Wassenaar, there were a number of points I would like to have cleared up about that, I think, for the record.

It should also be noted that H.R. 850, the SAFE Act, is completely consistent with Wassenaar's. It was inferred that maybe it wasn't. Somehow, it would violate the Wassenaar Arrangement. It does not at all. In fact, it allows for the very kind of review process that Wassenaar calls for.

It contains, among other things, a provision that gives the Secretary of Commerce a one-time, 15-day technical review of all crypto products prior to export. Second, it allows the President to stop exports to terrorist nations and to impose embargoes. And, third, it provides the Secretary of Commerce with the ability to stop the export of specific encryption products to specific individuals or organizations in specific countries if there is substantial evidence that such products will be used for military or terrorist purposes.

So the bill itself is completely consistent with Wassenaar. I think that ought to be on the record here today.

Thank you.

Mr. SHIMKUS. Mr. Holahan, did you want to follow up?

Mr. HOLAHAN. Just in terms of companies marketing themselves as being able to sidestep U.S. regulations, it is actually different from the companies actually flourishing. Someone like Siemens, they don't flourish because U.S. export restrictions—I can't speak for them. But an awful lot of people would say, we have got, you know, strong crypto outside of the States. You can actually get a freeware and shareware. Shareware and freeware companies don't flourish because of that. They may offer it.

But the question is, if used, people want it in American software products. The desktops of the world are populated by U.S. software products, and people do want it in the American products. Being able to offer it for free or a small amount of money will not cause us to flourish because of that. We have to offer something better than that. So the commercial argument is different from the actual technical argument.

Mr. SHIMKUS. We understand marketing.

Mr. HOLAHAN. Okay. So don't confuse the idea of having 650 products with actually some kind of a business market being out there, which is massively beyond belief, and we are all out there making tons of money just because we can develop crypto. Anyone can do that. That doesn't matter.

Mr. SHIMKUS. Does anyone else also want to add—I was also interested on the comments by Mr. Gillespie, the Wassenaar by Mr. Holahan. Anyone else want to add on the agreement?

Mr. HOLAHAN. Just on the Wassenaar, my term was it may violate the Wassenaar Arrangement. My point is that I would like to encourage—to perhaps look at if it sort of wouldn't violate——

Mr. TAUZIN. Would the gentleman yield? Where? Where might it violate Wassenaar?

Mr. HOLAHAN. Because if—my understanding of the act is that the Department of Commerce can regulate it. So if—for instance, there is no actual requirement to notify export of crypto above 64 bit or whatever it is that might do it or outside the 33 countries of Wassenaar.

I think there could be a few points whereby this might, you know, literally open the floodgates, rather than be contained, potentially. It depends on what way it is implemented.

Mr. HORNSTEIN. Can I point out Wassenaar is only for 33 countries? I mean, Israel is not a Wassenaar member, and they are not subject to the regulations of other countries, India and so on. So a lot of our serious competitors out there in the world are not subject to this regulation at all.

Mr. SHIMKUS. It has been a good panel, Mr. Chairman. I yield back the balance of my time.

Mr. TAUZIN. Thank the gentleman.

Mr. Hornstein, before we wrap, in regards to your comments about the handicaps to some of the contracting you are trying to engage in. Once the Commerce Department does, in fact, give you an export license, does Commerce Department regulations prevent you from servicing after the sale in any way or inhibit you from servicing after the sale?

Mr. HORNSTEIN. No. As Under Secretary Reinsch said, once you do get a license, then you would be able to support that.

Mr. TAUZIN. So there is no problem with servicing the contract once you get your export license and you do your sale. Your problem is in communicating prior to the award of the contract?

Mr. HORNSTEIN. Can I walk through a quick process with you?

Mr. TAUZIN. Quickly do that for me.

Mr. HORNSTEIN. No problem. You develop a product, and then you have to go for a review. Your engineers are developing it. They have got to keep the export people involved so we can actually go through, and it takes 90 to 120 days to get this product reviewed by Commerce.

Mr. TAUZIN. By Commerce.

Mr. HORNSTEIN. It goes out, and then you try to sell the product. Now you have a review. It is potentially—it may be exportable, it may not be, may be restricted or regulated. I now go out there. I have—most of the transactions I do are small deals, $25,000, $50,000. I am a billion dollar software company. Can you imagine 30 or 40 percent?

Mr. TAUZIN. Everyone takes that review.

Mr. HORNSTEIN. If I actually had to go through that sort of a process for a mass—I am selling mass market products. These are products that come off the store shelf and turnkey, and my consumers can use them for nonnefarious purposes.

Mr. TAUZIN. You don't have a general waiver on them. You have to go contract by contract?

Mr. HORNSTEIN. Correct, contract by contract.

Mr. TAUZIN. While your product is being reviewed, you are in the process of negotiating with the company who wants to buy it who is also negotiating with these foreign suppliers as well, right—well, maybe?

Mr. HORNSTEIN. I wouldn't file a license before I have a sale. Many times customers come to me and want the products that day, and there are other competitors out there. It takes 90 days or whatever period of time to get clearance from the Commerce Department.

Mr. TAUZIN. So even if you were able to clear all of these hurdles within the timeframes, your competitors have no such hurdles?

Mr. HORNSTEIN. Exactly.

Mr. TAUZIN. They can sell that day to the purchaser?

Mr. HORNSTEIN. Baltimore, based out of Ireland and the UK, has no restrictions whatsoever.

Mr. TAUZIN. Mr. Holahan, do you do that? Can you sell on a——

Mr. HOLAHAN. The way we regulate what is under Wassenaar and the European Union and the national legislation, that we actually allowed certain products to be exported on a notification basis.

Mr. TAUZIN. So you just notify them and then export?

Mr. HOLAHAN. Correct.

Mr. TAUZIN. You have no review process? You don't have to wait for anyone to say it is okay?

Mr. HOLAHAN. There is a continuing review process.

Mr. TAUZIN. Nobody has to tell you it is okay?

Mr. HOLAHAN. Okay.

Mr. TAUZIN. You can just notify and sell?

Mr. HOLAHAN. Correct.

Mr. TAUZIN. He has to go through an okay process.

Mr. HOLAHAN. Actually, I contest that, because Network Associates have bought two non-U.S. companies who are quite capable of exporting. My understanding, correct me——

Mr. HORNSTEIN. I can't export anything. All of my engineers are in the United States.

Mr. HOLAHAN. Do you have PGP engineers in Europe?

Mr. HORNSTEIN. No, PGP is in United States.

Mr. HOLAHAN. In Holland, no?

Mr. HORNSTEIN. No. I just have my sales people out there.

Mr. HOLAHAN. My understanding is that PGP is available internationally, downloaded free of charge, and that is outside the U.S.; is that right?

Mr. HORNSTEIN. That is correct.

Mr. TAUZIN. But his engineers are here, and you can't communicate before the sale; is that the problem?

Mr. HORNSTEIN. Correct.

Mr. HOLAHAN. Actually, I would contest. I think the term in the contract is render technical assistance in the development of products. I think you can actually market products outside the States. You can say, this product does this, this, this, and this. You can't get an engineer to help someone that is outside of the States. So, as far as we see, U.S. companies are able to market the products. If someone wants to build a product, they can't render engineering assistance——

Mr. HORNSTEIN. I can market, but most of my marketing is done by my borrowers who are international people. And for me to give them a demonstration version is another violation of the U.S. laws.

Mr. TAUZIN. I think we have the picture.

Mr. HOLAHAN. I am not arguing for those certain things. I am not trying to stop him from competing. But I think a demonstration of a product is actually allowed under the current legislation——

Mr. HORNSTEIN. As long as it is under my control and a controlled environment. I don't install it. My customers——

Mr. TAUZIN. There are a type of restrictions on which you can or cannot do?

Mr. HOLAHAN. I would agree with that.

Mr. TAUZIN. Right.

Mr. Dawson, do you want to add something before we wrap?

Mr. DAWSON. Quickly. By way of a quick walk-through, there is no prior approval required with the approach that we have implemented under the current resolution.

Mr. TAUZIN. Because Commerce has approved it?

Mr. DAWSON. Commerce has approved this, and there is no—our customers have no preapproval. It is preapproved for any customer, and they simply have to register themselves on our website, not with the U.S. Department of Commerce. So that is within the current regulations, et cetera. So I think it works, and I think it works without——

Mr. TAUZIN. But only people using your product?

Mr. DAWSON. Only people that are using that technique.

Mr. TAUZIN. That technique. That is correct.

Mr. Schultz.

Mr. SCHULTZ. If I can, just for 1 more second. Just with respect to law enforcement, I would like to give some encouragement in that area. If we relax our current encryption restrictions, there will be ways of getting keys even if the crypto is stronger.

Look at the Walker spy case, right? People reveal keys. We must always keep in mind the role of people in any technology. That is very important. That means one person in an organization that is using crypto for criminal purposes may be aware of that key and reveal the key. We must never lose the fact that we always have a very strong potential form of control.

And, second of all, with respect to crypto, we have heard somebody from the NSA tell us that, yeah, they monitor what goes on out there. And now some special vigilante organization that is very scary starts encrypted traffic lot using strong encryption. That is a heads-up. There are signs, there are telltales that the law enforcement community will get from the use of stronger encryption that will enable them——

Mr. TAUZIN. Mr. Schultz, that makes my point; and that is it is not sufficient for FBI purposes that NSA have that capability. FBI has to have its own capability, and that is the reason why the lab language, and perhaps we need to talk more about that. If we are going to successfully pass a bill that relaxes these export restrictions and, in fact, encourages stronger and stronger encryption products, which I support, we are going to have to make sure that there is strong cooperation between the industry and the manufacturers and the product developers and the FBI in terms of a lab

that gives them capability to serve this country's needs in terms of catching the bad guys when they are out there using those products.

Mr. Hornstein.

Mr. HORNSTEIN. Can I just give a couple of examples?

Network Associates in the past couple of years has worked very closely with the FBI. In the last year, I had 12 different meetings and conversations with different agencies.

Mr. TAUZIN. That is what I am talking about.

Mr. HORNSTEIN. For instance, you have heard of the Melissa virus potentially.

Mr. TAUZIN. Of course.

Mr. HORNSTEIN. The moment the Melissa virus was discovered, Network Associates worked very, very closely with the FBI, not only detecting and cleaning and decrypting the virus but we also worked with the FBI in assisting them on backtracking and locating the person who was out of I think it was New Jersey. And we worked very closely with them, the Remote Explore Virus.

Mr. TAUZIN. I think the FBI gave some credit to the industry for its assistance.

Again, thank you for that. That is exactly what we are going to be looking for if we can develop successful legislation.

Mr. HORNSTEIN. I guess my point is, for a company like Network Associates, which is trying to grow a security company, we are a global company, not a local company; and for us to remain viable and to be able to provide support to the FBI, we need to build and grow as a business. If our business isn't growing, we will lose our engineers.

Mr. TAUZIN. This has been an excellent discussion. I will just reaffirm, Mr. Markey and I have always been able to appreciate and enjoy James Joyce. What I can't appreciate and enjoy is that 7 million word Tax Code, and if any one of you can decipher that book, I would be happy.

Let me thank you very much. It has been very enlightening. We may call upon some of you again as we move toward our retreat. We want to understand a great deal more of some of—you raised some extraordinary problem areas for us in your testimony, with Mr. Arnold and Mr. Schultz, that I want to pursue further. We may want to come back to you with some additional questions.

And, all of you, your written record is a part of the record by unanimous consent. All members' written records are a part of the record. And the Chair will grant 30 days for anyone to submit additional and other information for the record.

Mr. Gillespie, you have the article from Mr. Cox that will be made a part of the record, as well as my letter from the Louisiana Sheriff's Association. Without objection, so ordered.

[The information referred to follows:]

[March 27, 1999—San Jose Mercury News]

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 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 Republicans 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, 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 eat 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, 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 super-

vises and approves all networks, and it 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.

LOUISIANA SHERIFFS' ASSOCIATION
May 17, 1999

The Honorable JOHN C. COOKSEY
U.S. House of Representatives
434 Cannon House Office Building
Washington, D.C. 20515

DEAR CONGRESSMAN COOKSEY: I am writing today to call your attention to H.R. 850, the SAFE Act, which will be heard tomorrow in the International Economic Policy & Trade subcommittee of the International Relations Committee. This legislation deals with issues that are of some concern to the sheriffs in Louisiana and law enforcement in general. I hope that you will work to prevent any weakening amendments and report this bill favorably to the full House of Representatives.

Our association passed the enclosed resolution last year in opposition to a proposal that would have "escrowed" encryption keys for use by the government. This resolution speaks to the concerns and problems that such a proposal would create. This year we are seeking to guarantee the security of encryption by preventing the government from taking such steps as "escrowing" encryption keys. That is why we need H.R. 850 passed favorably without any amendments.

Please review the enclosed resolution and support H.R. 850 in the subcommittee hearing tomorrow. Should you have any questions regarding this issue, please contact me at the number above.

Sincerely,

A.R. "TREY" HODGKINS, III
Manager of Governmental Relations

RESOLUTION

WHEREAS, In today's digital age, individuals, private organizations and government agencies store and transmit ever-increasing amounts of confidential information within and over computer and telecommunications networks; and

WHEREAS, This activity necessitates that individuals, organizations and agencies need to protect their confidential information with the strongest available computer encryption technology to deter access or theft of this information; and

WHEREAS, Without powerful encryption security in Louisiana's information networks, the computer and telecommunications systems that control such critical law enforcement functions as communication and emergency response, as well as the vital services providing air traffic control, financial systems, the power grid and the public telephone system would become vulnerable to attack from high tech terrorists; and

WHEREAS, The confidential nature of a number of law enforcement functions, including investigative evidence keeping, witness information and prison and corrections records keeping would also be vulnerable to unauthorized access without these powerful encryption systems; and

WHEREAS, Legislation proposed by the Federal Bureau of Investigation would require all users of encryption to deposit a key with a "key escrow" agent that would be available to FBI access; and

WHEREAS, This FBI access would create and maintain a dangerous and unnecessary vulnerability to Louisiana's information and computer infrastructure while failing to offer any increased level of protection these systems require; and

WHEREAS, While the FBI's efforts toward recovering information about criminal access to high security encryption are well intentioned, the "key escrow" plan poses too many severe threats to public safety, confidentiality and legitimate computer users that far outweigh the isolated benefits it may provide; and

WHEREAS, *Americans for Computer Privacy* is a broad-based national coalition of groups representing law enforcement, industry, taxpayers, financial institutions, civil liberties and online commerce dedicated to ensuring that all Americans are permitted to protect their privacy with the strongest possible encryption without mandatory government access to information; now, therefore, be it

RESOLVED, That the Louisiana Sheriffs' Association, at it's meeting on May 20, 1998 registers its' opposition to any compromise to the security and privacy that strong encryption affords the ability of law enforcement to provide public safety, and, be it further

RESOLVED, That the Louisiana Sheriffs' Association wishes to become an active member of the *Americans for Computer Privacy* coalition and win devote any available resources to passage of pro-computer privacy legislation and opposing any "key escrow" mandates; and

RESOLVED, That the Louisiana Sheriffs' Association wishes that a copy of this resolution be sent to each member of the Louisiana Congressional Delegation.

CERTIFICATION

This is to certify that the above and foregoing is a resolution adopted by the Executive Board of the Louisiana Sheriffs' Association on May 20, 1998.

DATE 5-20-98

R.B. "BUCKY" RIVES, JR.
Executive Director

Mr. TAUZIN. The hearing stands adjourned. Thank you very much.

[Whereupon, at 12:50 p.m., the subcommittee was adjourned.]

[Additional material submitted for the record follows:]

PREPARED STATEMENT OF HON. BOB GOODLATTE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF VIRGINIA

Mr. Chairman, I would like to thank you for holding today's important hearing on legislation I have introduced—H.R. 850, the Security and Freedom through Encryption (SAFE) Act of 1999—to encourage the use of strong encryption.

This much-needed, bipartisan legislation, which currently has 255 cosponsors, including a majority of the Republican and Democratic leadership, three-fifths of the members of the Commerce Committee, and over two-thirds of the members of this Subcommittee, accomplishes several important goals. 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. The SAFE Act, by allowing all Americans to use the highest technology and strongest security available, will provide them with that confidence.

Third, with the availability of strong encryption overseas and on the Internet, our export controls 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.

Removing these export barriers will free U.S. industry to remain the leader in software, hardware, and Internet development. And by allowing our computer industry to market the highest technology with the strongest security features available, America will lead the way into the 21st century Information Age.

This bipartisan legislation enjoys the support of members and organizations across the entire spectrum of ideological and political beliefs. The SAFE Act enjoys this support 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.

The Administration is proposing an Industrial Age solution to an Information Age problem. The SAFE Act, on the other hand, prevents 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, the SAFE Act ensures that all Americans have the right to choose any security system to protect their confidential information.

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. That is precisely what the SAFE Act will ensure. I urge each of my colleagues to support this bipartisan legislation, and thank you for holding today's hearing.

GLOBAL INTEGRITY
WEST LAFAYETTE, IN 47906-1182
June 1, 1999

The Honorable W.J. TAUZIN
Chair
Committee on Commerce
U.S. House of Representatives
316 Ford Building
Washington, DC 20515

DEAR REPRESENTATIVE TAUZIN: In response to your request for additional information at the Committee on Commerce hearing on H.R. 850 last Tuesday, I am pleased to submit this letter.

Your first question was whether the cryptographic product (SmartGate) described at the hearing by Mr. David Dawson of V-ONE corporation provides a solution for the concerns associated with relaxation of current U.S. encryption export restrictions. After visiting the V-ONE web site and reading the descriptions of V-ONE's SecureGate product, I learned that this product provides encryption for pager devices using Triple-DES (a reasonably strong encryption algorithm). It was certainly generous of Mr. Dawson to offer to share the code used to implement this product. On the other hand, SecureGate is a rather specialized product that does not address many of the issues discussed at last week's hearing. This product does not, for example, encrypt network links to web servers, nor does it help in securing telecommunications links. As such, SecureGate does not provide a sufficiently general solution—the kind of solution, unfortunately, that would be needed to address the many issues related to U.S. encryption export controls.

Your second question was whether prohibitions against mandatory key recovery would discourage voluntary key recovery. It seems to me that the critical issue here is not the relationship between the two, but rather the particular party that would be in charge of voluntary recovery. If the U.S. Government establishes the role of voluntary key recovery agent and postures itself accordingly, I am confident that the result would be firm resistance even to voluntary key recovery. The fiasco with the Clipper Chip and Capstone should by now have taught us that not only U.S. commercial entities, but also especially foreign organizations are less than enthusiastic about the U.S. Government serving in the role of key recovery agent. In short, few organizations trust the Government and its potential intentions sufficiently. If, on the other hand, commercial entities continue to provide key recovery services on a widespread basis, I am confident that the negative reaction towards voluntary key recovery will in general soften over time.

The only possible link between prohibition of mandatory key recovery and the popularity of voluntary key recovery might result from the inference that somehow since the U.S. Government prohibits mandatory key recovery, something must be wrong with key recovery in general (regardless of whether it is mandatory or voluntary). I do not, however, believe that such an inference is sufficiently logical to be held widely among those who are considering key recovery solutions.

Thank you for allowing me to serve the Commerce Committee. I look forward to the possibility of working with you and the others on this Committee in the future should your needs so dictate. I am in particular eager to explain the concept of an "encryption culture" and to show its bearing on H.R. 850.

Sincerely yours,

E. EUGENE SCHULTZ, PH.D., CISSP
Trusted Security Advisor and Research Director