S. HRG. 104–499

ECONOMIC ESPIONAGE

HEARING

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE
UNITED STATES SENATE

AND THE

SUBCOMMITTEE ON TERRORISM, TECHNOLOGY, AND GOVERNMENT INFORMATION

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED FOURTH CONGRESS

SECOND SESSION

FEBRUARY 28, 1996

Serial No. J–104–75
(Senate Committee on the Judiciary)

Printed for the use of the Select Committee on Intelligence of the United States Senate and the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
25–063 CC WASHINGTON : 1996

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-052862-3

S. HRG. 104–499

ECONOMIC ESPIONAGE

HEARING

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE UNITED STATES SENATE

AND THE

SUBCOMMITTEE ON TERRORISM, TECHNOLOGY, AND GOVERNMENT INFORMATION

OF THE

COMMITTEE ON THE JUDICIARY UNITED STATES SENATE

ONE HUNDRED FOURTH CONGRESS

SECOND SESSION

FEBRUARY 28, 1996

Serial No. J–104–75
(Senate Committee on the Judiciary)

Printed for the use of the Select Committee on Intelligence of the United States Senate and the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
25–063 CC WASHINGTON : 1996

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-052862-3

SELECT COMMITTEE ON INTELLIGENCE

ARLEN SPECTER, Pennsylvania, *Chairman*
J. ROBERT KERREY, Nebraska, *Vice Chairman*

RICHARD G. LUGAR, Indiana
RICHARD C. SHELBY, Alabama
MIKE DEWINE, Ohio
JOHN KYL, Arizona
JAMES M. INHOFE, Oklahoma
KAY BAILEY HUTCHISON, Texas
CONNIE MACK, Florida
WILLIAM S. COHEN, Maine

JOHN GLENN, Ohio
RICHARD H. BRYAN, Nevada
BOB GRAHAM, Florida
JOHN F. KERRY, Massachusetts
MAX BAUCUS, Montana
J. BENNETT JOHNSTON, Louisiana
CHARLES S. ROBB, Virginia

ROBERT DOLE, Kansas, *Ex Officio*
THOMAS A. DASCHLE, South Dakota, *Ex Officio*

CHARLES BATTAGLIA, *Staff Director*
CHRISTOPHER C. STRAUB, *Minority Staff Director*
KATHLEEN P. MCGHEE, *Chief Clerk*

COMMITTEE ON THE JUDICIARY

ORRIN G. HATCH, Utah, *Chairman*

STROM THURMOND, South Carolina
ALAN K. SIMPSON, Wyoming
CHARLES E. GRASSLEY, Iowa
ARLEN SPECTER, Pennsylvania
HANK BROWN, Colorado
FRED THOMPSON, Tennessee
JON KYL, Arizona
MIKE DEWINE, Ohio
SPENCER ABRAHAM, Michigan

JOSEPH R. BIDEN, JR., Delaware
EDWARD M. KENNEDY, Massachusetts
PATRICK J. LEAHY, Vermont
HOWELL HEFLIN, Alabama
PAUL SIMON, Illinois
HERBERT KOHL, Wisconsin
DIANNE FEINSTEIN, California
RUSSELL D. FEINGOLD, Wisconsin

MARK R. DISLER, *Chief Counsel*
MANUS COONEY, *Staff Director and Senior Counsel*
CYNTHIA C. HOGAN, *Minority Chief Counsel*
KAREN A. ROBB, *Minority Staff Director*

SUBCOMMITTEE ON TERRORISM, TECHNOLOGY, AND GOVERNMENT INFORMATION

ARLEN SPECTER, Pennsylvania, *Chairman*

FRED THOMPSON, Tennessee
SPENCER ABRAHAM, Michigan
STROM THURMOND, South Carolina

HERBERT KOHL, Wisconsin
PATRICK J. LEAHY, Vermont
DIANNE FEINSTEIN, California

RICHARD A. HERTLING, *Chief Counsel*
JON LEIBOWITZ, *Minority Chief Counsel and Staff Director*

CONTENTS

ECONOMIC ESPIONAGE

WEDNESDAY, FEBRUARY 28, 1996

U.S. SENATE,
SELECT COMMITTEE ON INTELLIGENCE, AND THE
SUBCOMMITTEE ON TERRORISM, TECHNOLOGY, AND
GOVERNMENT INFORMATION,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Joint Committees met, pursuant to notice, at 10:47 a.m., in room SD–106, Dirksen Senate Office Building, the Honorable Arlen Specter, Chairman of the Select Committee on Intelligence, presiding.

Present: Senators Specter, Shelby, Kyl, Kohl, Kerrey of Nebraska, Leahy, Baucus, Johnston, and Feinstein.

Also Present for the Intelligence Committee: Charles Battaglia, Staff Director; Chris Straub, Minority Staff Director; Suzanne Spaulding, Chief Counsel; and Judy Hodgson, Acting Chief Clerk.

Also Present for the Judiciary Subcommittee: Richard A. Hertling, Chief Counsel; Jon Leibowitz, Minority Chief Counsel; and Victoria Bassetti, Minority Counsel.

Chairman SPECTER. This Joint Hearing of the Senate Select Committee on Intelligence and the Judiciary Subcommittee on Terrorism, Technology, and Government Information, will now proceed.

We have called this hearing to discuss the emerging threat to the U.S. economic and national security posed by economic espionage. Economic espionage involves, among other things, the theft through covert means of vital proprietary economic information owned by U.S. businesses and critical to sustaining a healthy and competitive national economy.

Senator Kohl, the distinguished ranking member of the Terrorism subcommittee, and I recently introduced two bills to combat economic espionage by foreign governments, their agents, and others.

I have a rather lengthy statement which will be placed in the record, without objection.

OPENING STATEMENT OF SENATOR ARLEN SPECTER

This joint hearing of the Senate Select Committee on Intelligence and the Judiciary Subcommittee on Terrorism, Technology, and Government Information has been called to discuss the emerging threat to the U.S. economic and national security posed by economic espionage. Economic espionage involves, among other things, the theft through covert means of vital proprietary economic infor-

mation, owned by U.S. businesses and critical to sustaining a healthy and competitive national economy. Senator Kohl and I recently introduced legislation to combat economic espionage by foreign governments, their agents and others.

The White House Office of Science and Technology is reported to have estimated losses to U.S. businesses from foreign economic espionage at nearly $100 billion per year; ABC News recently reported that American job losses are estimated to be over 6 million this decade due to economic espionage. Further, the U.S. Government will spend nearly $2 trillion this decade on basic research; basic research, due to its unprotected status under intellectual property concepts, is the No. 1 target of foreign countries and companies who do not invest in basic research.

Economic espionage has a devastating impact upon innovation. Our second panel of witnesses this morning will discuss how their particular innovations have been targeted, and the resulting impact upon their businesses and lives. It is reasonable to note that these witnesses, in coming forward and admitting they have been targeted and victimized, are the rare exception to the general practice among American business of not "airing their dirty laundry" in public.

The development and production of proprietary economic information is an integral part of U.S. business and is thus essential to preserving the competitiveness of the U.S. economy. Because of the importance attached to our national competitiveness, current U.S. policy is to treat economics as a national security issue. In this regard, the February 1995 White House National Security strategy focused on economic security as a national security priority, and identified economic revitalization as one of the three central goals of the United States. Secretary of State Warren Christopher stated in testimony before the Senate Foreign Relations Committee that, "In the post-cold war world, our national security is inseparable from our economic security."

Foreign governments, their agents, and corporations actively target U.S. persons, firms, industries, and the U.S. Government itself to steal critical information in order to provide their own industrial sectors with a competitive advantage. A recent example involves Russian President Boris Yeltsin, who on February 7, 1996, ordered top Russian officials to close the technology gap with the West and told them to make better use of industrial intelligence to do so. Experts note that there are 51 countries that have spies that are active in the United States and who count economic intelligence gathering among their targeting. Current FBI investigations reflect 23 countries actively engaged in economic espionage activities against the United States. Our first witness, FBI Director Louis Freeh, will address these and other issues relating to this emerging national security threat.

U.S. espionage statutes and other Federal criminal statutes do not cover many current economic intelligence-gathering operations. Since no Federal statute directly addresses economic espionage or the protection of proprietary economic information in a thorough, systematic manner, investigators and prosecutors have attempted to combat the problem by using existing laws, all of which were de-

signed to counteract other problems. Examples are the wire fraud and mail fraud statutes.

Another problem with existing law is that it fails to provide confidentiality to the information in question during criminal and other legal proceedings. Proprietary economic information derives value from its confidentiality; if this is lost during legal proceedings, then the value of the information is greatly lessened. Rather than risk such compromise, an owner may not attempt to enforce their legal rights.

In conclusion, only by providing for a mechanism to protect U.S. proprietary economic information from foreign theft can we hope to maintain our economic edge, and thus preserve our national security.

Welcome to our witnesses this morning. We look forward to their testimony and other materials that have been received for the record.

I turn now to Senator Kohl, the ranking member of the subcommittee, and then to Senator Kerrey.

Chairman SPECTER. We have very distinguished witnesses today. The Director of the FBI, Louis Freeh; the former president of Ellery Systems, Inc., Geoffrey Shaw; Dr. Raymond Damadian, president and chairman of Fonar Corporation; and there are some others who will be available for questioning.

So in order to proceed expeditiously, I will now yield to my distinguished ranking member on the Judiciary Subcommittee, Senator Kohl.

OPENING STATEMENT OF SENATOR KOHL

I thank you, Mr. Chairman.

Today, Mr. Chairman, a piece of information can be as valuable to a business as in fact a factory is. The theft of that information can do more harm than if an arsonist torched that factory. But our Federal criminal laws do not recognize this and do not punish the information thief. This is unacceptable and we are here today to begin remedying the problem.

Today the real American economic miracle is its innovation, its ideas, and its information. We must protect them from theft as vigorously as we would the invention of the cotton gin, the telephone, and the steam engine. We have done a good job protecting people when all their hard work produces something tangible like machines or hardware. The time has come to protect the people who produce information and ideas.

Mr. Chairman, this protection is crucial. Most Americans probably do not realize that an employee could walk out of his company with a copy if its customer list, its suppliers list, and all of its pricing information, and sell that information to the highest bidder, with virtual impunity. Yet 3 years ago in Arizona an engineer for an automobile air bag manufacturer was arrested for doing just that—selling his company's manufacturing design, strategies, and plans. He asked the company's competition for more than a half a million dollars, to be paid in small bills. And he sent potential buyers a laundry list of information they could buy. Five hundred dollars for the company's capital budget plan, $1,000 for a small piece of equipment, and $6,000 for planning and product documents. The

company was lucky the theft of its information occurred in Arizona, which is only 1 of 20 States that allow prosecution for this kind of arrest—of theft. But if that many had been in 1 of 30 other States in our country, he could not have been accused of any crime.

It is even more threatening to our country's economic security when that theft is masterminded by a foreign government determined to loot our economic competitiveness. And shockingly, that type of piracy is all too commonplace today.

To explain just how threatening this foreign theft can be, let me say that just last year a former employee of two major computer companies admitted to stealing vital information on the manufacture of microchips and selling that information to China, Cuba, and Iran. For almost a decade, he copied manufacturing specifications, information worth millions of dollars. Armed with that, the Chinese, Cubans, and Iranians have been able to close the gap on our technology leads.

Late last year the FBI arrested this man and charged him under the Federal stolen property and mail fraud laws. But it appears that the charges may be a bit of a stretch, because he did not actually steal tangible property—he only stole ideas, and our Federal law does not cover mere ideas.

The problem of foreign economic espionage will only increase. Even as the cold war ended, our former enemies and our current allies began retooling their intelligence agencies. They have turned their vast spying apparatus on us, on our businesses, on the very ideas and information that keep this country safe. Foreign governments look at America and see a one stop shopping mall for all their business and information needs. What they cannot buy legitimately, they will shoplift.

Because of the gap in our law, Senator Specter and I have jointly introduced two bills that will put a stop to this. The only difference between the two proposals is that the Industrial Espionage Act does not require prosecutors to prove that a foreign government sponsored the theft of the information. In other words, any person or company, foreign or domestic, who steals this information, would be able to be prosecuted. We believe this measure is vitally needed because stealing proprietary information should be prosecuted regardless of whether a foreign government or an American citizen committed this crime. The business destroyed because of an information thief does not care whether the thief was French, Chinese, or American, nor should our criminal law.

We have carefully drafted these measures to ensure that they can only be used in flagrant and egregious cases of information theft. We do not want this law to be used to stifle the free flow of information.

Mr. Chairman, these two measures should be a top bipartisan priority. The longer we wait, the more we leave ourselves vulnerable to the ruthless plundering of our country's vital information. But with the FBI and the Administration's help, we should be able to move these proposals along.

I thank you, Mr. Chairman, and it is good to be here today.

Chairman SPECTER. Thank you very much, Senator Kohl.

Now I would like to yield to the distinguished ranking member of the Intelligence Committee, Senator Kerrey.

Vice Chairman KERREY. Thank you, Mr. Chairman.

First of all, I want to congratulate both you and Senator Kohl for holding this hearing and for introducing your legislation. I would welcome Louis Freeh as our first witness and indicate that this is a matter that has given a lot of us a great deal of concern, and it is not an easy problem for us to solve. The question of whether or not we need to change our law has been presented now to us by both Senator Specter and Senator Kohl, and it may, in fact, be that our laws need to be changed. There's no question that we are at risk both on the government side; that is to say from governments, as well as on the private sector side. And there's no question as well that this is one of those problems that unfortunately stays outside of our view. I'm in business myself and I'm very sympathetic to the problem faced by businesses who may not want to disclose that a theft has happened. This should be regarded by Americans as a serious problem both for national security and to national competitiveness, something that could jeopardize jobs and standards of living and our own ability to be able to keep America safe and free.

So I appreciate very much, Mr. Chairman, your holding the hearing and look forward to the witnesses testimony.

OPENING STATEMENT OF VICE CHAIRMAN KERREY

Mr. Chairman, I commend you and Senator Kohl for directing the Senate's attention today to a serious problem, a problem which may well be soluble by making law and enforcing law. I am in business myself and I understand why the victims, those whose proprietary information is stolen from them, are often reluctant to make their losses public. Consequently, intellectual property theft is one of those silent crimes, generally out of the public eye, but a crime which threatens our national security as well as the ability of U.S. business to compete in the world.

This is a national security problem on several levels. First, we have to counter foreign government efforts to steal our advanced technology—of course, our defense and intelligence technology, but also the advanced computing and communications technologies that are essential both to defense and to economic competitiveness. But intellectual property theft, if left unchecked, could also have a more corrosive effect on our security. We will become known as a country which doesn't protect proprietary information and intellectual property. If we don't establish firm protections, the United States will gradually cease to be a center of creativity and invention, and our national power will slip away.

We want the world to come here and invent and invest because America is the safest place in the world to profit from one's own bright idea. If this hearing can point in that direction, it will be a morning well spent.

Chairman SPECTER. Thank you very much, Senator Kerrey. Senator Kyl, would you care to make an opening statement?

Senator KYL. Thank you, Mr. Chairman.

As a member of both the Judiciary Committee and the Intelligence Committee, let me compliment both you and Senator Kohl for bringing this legislation——

Chairman SPECTER. You can have twice as much time, Senator.

Senator KYL. Well, I'll take half as much, how would that be. But looking forward to Director Freeh's testimony. And again compliment you for bringing this important legislation before the committees.

Thank you.

Chairman SPECTER. Thank you very much, Senator Kyl.

Senator Leahy.

Senator LEAHY. Mr. Chairman, I'll put my full statement in the record, but I think that this is an extremely important issue. I'm concerned about the vulnerability of so much of our trade secret proprietary information. We have a great deal of our normal commerce today in fact, conducted via computers. We oft times transmit confidential proprietary information by computers talking to computers. We need far better encryption. We need far better laws to go after people who steal. Last summer I introduced, along with Senators Kyl and Grassley, the National Information Infrastructure Protection Act, to increase the protection for computers, both government and private, and the information on those computers from the growing threat of computer crime. We all know what to do when we hear about somebody who pulls up in a car, rushes into a bank, guns blazing, robs the bank and takes off. We think of the 20 to 30 to 40 thousand dollars that the robbers might have gotten in that kind of an episode. But I think we have to be far more worried about the 200, 300, 400 million dollars that may be stolen at 3 o'clock in the morning by tapping computer keys. This is extremely important. I'd ask that my whole statement be made a part of the record.

Chairman SPECTER. It will be made part of the record without objection, Senator Leahy.

[The prepared statement of Senator Leahy follows:]

PREPARED STATEMENT OF SENATOR PATRICK LEAHY

Spying on American companies in order to obtain their trade secrets and confidential proprietary information is—to put it bluntly—stealing. Although the estimates of how much this stealing costs our Nation's business and our economy are rough, the range is in the billions of dollars per year.

Unfortunately, the problem appears to be growing. The increasing dependence of American industry on computers to store information and to facilitate communications with customers, suppliers and far-flung subsidiaries, presents special vulnerabilities for the theft of sensitive proprietary information.

I have long been concerned about this vulnerability. That is why, last summer, I introduced with Senators Kyl and Grassley the National Information Infrastructure Protection Act (S. 982) to increase protection for computers, both government and private, and the information on those computers, from the growing threat of computer crime. Business dependency on computers and the growth of the Internet are both integrally linked to people's confidence in their security and privacy. That is why I have been working over the past decade to create a legal structure to foster both privacy and security.

The bills we consider here today reflect significant efforts to better protect our industrial lifeblood—the imaginative ideas and the special know-how that give American companies the edge in global competition.

I look forward to exploring some of the issues raised by these bills. We need to be clear about where the gaps in current law are that need remedying by a new criminal law. We also need to be assured that under these bills, a garden variety dispute between a former employee and a company over customer list information, which commonly is handled by our State courts, does not tie up Federal law enforcement and Federal court resources. Finally, we need to know what the repercussions will be in our relations with our allies if we threaten 25-year jail terms for foreign operatives who engage in economic espionage.

But enacting new criminal laws—even those that threaten huge jail terms—for stealing trade secret and proprietary information and for breaking into computers to steal sensitive electronic information, are not the whole answer. These criminal laws often only come into play too late, after the theft has occurred and the injury inflicted.

We should also be encouraging American firms to take preventive measures to protect their vital economic information. That is where encryption comes in. Just as we have security systems to lock up our offices and file drawers, we need strong security systems to protect the security and confidentiality of business information. Encryption enables all computer users to scramble their electronic communications so that only the people they choose can read them.

A recent report by the Computer Systems Policy Project, which is a group of CEOs from 13 major computer companies, estimates that, without strong encryption, financial losses by the year 2000 from breaches of computer security systems to be from $40 to $80 billion. The estimated amount of these losses is staggering. Unfortunately, some of these losses are already occurring. The report quotes one U.S. based manufacturer, who said:

> We just lost a major . . . procurement in [a Middle-Eastern country] by a very small margin to [a State subsidized European competitor]. We were clearly breached; our unique approach and financial structure appeared verbatim in their competitor's proposal. This was a $350 million contract worth over 3,000 jobs.

Yet another U.S. based manufacturer is quoted in the report, saying:

> We had a multi-year, multi-billion dollar contract stolen off our P.C. (while bidding in a foreign country). Had it been encrypted, [the foreign competitor] could not have used it in the bidding timeframe.

We are going to hear today from witnesses who can add to our understanding of how this problem can inflict serious damage on our economy.

Encryption is not only good for American business, it should be good business for Americans. Our computer companies are the leaders in the world in encryption technology. Short-sighted government policy is holding them back. Our current export restrictions on encryption technology are fencing off the global marketplace and hurting the competitiveness of this part of our high-tech industries. While national and domestic security concerns must weigh heavily, we need to do a better job of balancing these concerns with American business' need for encryption and the economic opportunities for our hi-tech industries that encryption technology provides.

There is an ongoing advertising campaign for "The Club", a device that you hook over the steering wheel of your car to deter car theft. The ads all say that police recommend the Club. Perhaps we would have more success in fighting economic espionage if, in addition to strong criminal sanctions, we had a similar campaign urging American companies to use strong encryption.

Next week, I hope to join with a number of colleagues to introduce a bill that addresses some of my concerns about encryption. I look forward to working with the Chairman and hope that he will hold hearings on this important matter.

Chairman SPECTER. Senator Feinstein.

OPENING STATEMENT OF SENATOR FEINSTEIN

Thank you very much, Mr. Chairman.

I'd like to join my colleagues in thanking you and Senator Kohl. Probably no State will be more benefited by your legislation than mine. California has one-third of all of the high-tech in the Nation. I think Silicon Valley is well-known, as well as the San Diego area, for that.

I'd like to just very briefly give you three examples of the kind of theft that you are attempting to get at that recently happened in California. A group of suspects downloaded a copy of a San Jose company's proposal to NASA onto their laptops, and they moved to New Mexico. Using this information, the person or persons then prepared the winning bid for a multimillion-dollar NASA contract. The U.S. Attorney's office subsequently refused to approve a warrant for their arrest because of court holdings that information

such as this was not goods, wares or merchandise under the Interstate Transportation of Stolen Property Act.

Second, in Palo Alto, a French national, after submitting his resignation to his employer, entered the company after hours, downloaded proprietary computer source codes, packed his bags with the source codes in his suitcases, and left for the airport, where he was subsequently arrested.

Just last year there was the case of William Guidey, a systems engineer who worked for Intel Corporation and Advanced Microdevices, two California-based companies. According to the FBI, in Guidey's comments to the press, he took designs for making Intels 386 and 486 and Pentium microprocessors and passed it along to Cuba, North Korea, Iraq, China, Iran, the Soviet Union, and East Germany. He claims to have provided advanced microdevices technology to Cuba's M–6 technical espionage unit for nearly a decade. Guidey is currently under Federal indictment in northern California.

These are just three instances, happened fairly recently, in California, which I think demonstrate the value and worth of your legislation. So I would just like to say thank you very much.

Chairman SPECTER. Thank you very much, Senator Feinstein.

Senator Baucus.

Senator BAUCUS. Thank you, Mr. Chairman.

I have a statement I'd like to put in the record.

I think it's important to remind ourselves just how difficult this problem is. We're a nation of ideas. I think it's American ideas, American ingenuity, which have spawned most of the technology revolution that's occurred in the world, and I think that's going to continue. Other countries know that. They know the Americans are probably better than most people at coming up with new ideas.

The difficulty is, with advances in technologies, communications technologies and any technology, some people in our society have a hard time keeping up with advances. I think there's a lag, if you will, that in part is causing economic anxiety. It's causing anxiety in lots of American families, who just have a hard time keeping up. Their incomes are not keeping up in many respects.

In addition, it's hard for law enforcement to keep up with changes in technology. We all know about the problems of the $100 counterfeit bills. You know, it's sometimes difficult for law enforcement to stay ahead of those who want to take advantage of developments in technologies. That is, we wanted to develop a $100 bill that can't be counterfeited, but with advances in technology, it's easier and easier in the world today for a company or an individual to find the technology to counterfeit $100 bills that are very difficult to detect. That's just one example.

But in the case of economic espionage it's clear that the law has not kept up with technological advance. The law has not kept up with the ability of some unsavory people, if they want to, to take advantage of certain opportunities. And we just have to work harder in finding a way so that there's less of a lag between advances in technologies and society adjusting to them.

It is also not an easy problem to solve because the more we impose criminal sanctions, the more we potentially intrude upon the legitimate civil liberties of individuals. That's a very real concern.

I just remind all of us that, first, economic espionage is a very important problem we have to solve, but second, we have to do it very carefully so we're not going too far, in some respects causing even more problems than we're attempting to solve.

OPENING STATEMENT OF SENATOR MAX BAUCUS

Thank you Mr. Chairman. I commend you and the Vice Chairman for holding this very important hearing. I would also like to add that I am particularly pleased that it is being held in the open. The issue of foreign economic espionage is too important to be discussed behind closed doors.

The United States is a nation of ideas. Ideas are what enrich our political process. Ideas are the hallmarks of our educational institutions. Ideas that challenge complacent thinking involve virtually every American every day. More importantly, however, ideas form a basis for our economic competitiveness.

I do not need to recount here the important ideas that are part of American innovation, inventiveness, and ingenuity. People like the Wright Brothers, Edison, Ford, and, yes, information gurus like Bill Gates have helped spawn America's economic powerhouse. Yankee ingenuity is part of our heritage, and it is critical to our future economic well-being and thus important for our national security.

I believe that there is evidence to suggest that foreign governments and foreign government-owned corporations recognize that ideas form an essential pillar of America's economic power. Realizing this, they seek to take what is not theirs. This goes beyond a question of routine economic espionage. When a foreign government is involved, the espionage takes on a far more serious tone. With the full weight of a government's intelligence collection activities targeted against an American citizen or an American corporation, the so-called playing field is tilted drastically against us. This morning, our witnesses will give us some insights into how this is happening.

Also this morning, we will hear how our criminal statutes may not be adequate to confront this important national security problem. Perhaps through criminal prosecutions we will be able not only to punish but also to deter those who feel that America's ideas are easy targets. I believe today's testimony will help to form an important record so that the Congress can take the necessary steps to protect our interests—and American ideas.

Thank you, Mr. Chairman.

Chairman SPECTER. Thank you very much, Senator Baucus.

Senator Johnston.

Senator JOHNSTON. Mr. Chairman, as the world becomes increasingly competitive and increasingly technologically oriented, it is more important than ever that we protect our proprietary interests, our intellectual property, our technology, that we keep the world trading system fair. So I would just encourage you, you and Senator Kohl and others, who will lead this fight as far as the Congress is concerned. I would encourage the Administration to be much more vigilant, much more active, much more aggressive in keeping this world trading system fair.

To steal secrets is not fair, and we must be much, much more aggressive. We've got to change our laws. The FBI, the CIA, all, I think, need to be involved to an extent they have not been. Otherwise the unfairness of it will cost American jobs and cost America's place in the world trading market.

Chairman SPECTER. Thank you very much, Senator Johnston.

That has been, I think, a good statement of the intensity of the problem. I would add one or two other notes, that the White House Office of Science & Technology estimates losses to U.S. businesses from foreign economic espionage in the $100 billion range. And ABC News, which has done a very extensive analysis, has estimated that some six million job losses are attributed during this decade to economic espionage.

Earlier this month, on February 7, Boris Yeltsin, president of Russia, ordered top Russian officials to close the technology gap with the West and to make better use of industrial espionage. The FBI has quite a bit of information on this subject, so we now turn to the very distinguished director, Louis Freeh.

The floor is yours, Director Freeh.

TESTIMONY OF LOUIS FREEH

Director FREEH. Thank you, Mr. Chairman, and distinguished members of the panel. As always, it's a great privilege and honor to appear before the committee.

Mr. Chairman, I have prepared a somewhat lengthy statement. With your permission, I would submit that for the record.

Chairman SPECTER. Your full statement will be made a part of the record without objection. And to the extent you can summarize—you know the practices very well here—leave us the maximum time for dialog.

Director FREEH. OK, I'll try to do it in less than 5 minutes, if that's OK.

Chairman SPECTER. That would be terrific. Thank you.

[The prepared statement of Director Freeh follows:]

PREPARED STATEMENT OF LOUIS FREEH

ECONOMIC ESPIONAGE

Good morning Mr. Chairman and distinguished members of the committees. At the request of the committees, I am pleased to have this opportunity to appear before you to discuss economic espionage, and to provide examples of this serious assault on our nation's intellectual property and advanced technologies.

I am also pleased that the committees have had the opportunity to consult with Professor James P. Chandler from George Washington University. I had the pleasure of meeting with Professor Chandler last week. He makes a most compelling argument for legislation to address a problem that he estimates is costing American companies billions of dollars, with over a million jobs lost from stolen intellectual property. His reputation as a national expert on economic espionage is well deserved and I think the committee will find his written testimony most convincing.

The development and production of intellectual property and advanced technologies is an integral part of virtually every aspect of United States trade, commerce and business. Intellectual property, that is, government and corporate proprietary economic information, sustains the health, integrity and competitiveness of the American economy, and has been responsible for earning our nation's place in the world as an economic superpower.

The theft, misappropriation, and wrongful receipt of intellectual property and technology, particularly by foreign governments and their agents, directly threatens the development and making of the products that flow from that information. Such conduct deprives its owners—individuals, corporations and our nation—of the cor-

responding economic and social benefits. For an individual, a stolen plan, process or valuable idea may mean the loss of their livelihood; for a corporation, it could mean lost contracts, smaller market share, increased expenses and even bankruptcy; and, for our Nation, a weakened economic capability, a diminished political stature, and loss of our technological superiority. Most estimates place the losses to businesses from theft and misappropriation of proprietary information at billions of dollars a year.

Economic espionage is devastatingly harmful to the United States. Our nation has historically placed high value on the development and exploitation of our citizens' creativity. The framers of the constitution believed in this principle (see article 1, section, 8, clause 8: "To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors exclusive Right of their respective Writings and Discoveries.") While serving as Secretary of State, Thomas Jefferson provided the vision and leadership which resulted in Congress enacting the Patent Act of 1790. This act created an agency in the Department of State which administered the infant patent system, demonstrating the immense importance which the framers attached to the principle of intellectual property. Congress ordered that it be overseen by the Secretary of State, the Secretary of the Department of War and the Attorney General. Jefferson's views were revealed in a letter he penned to Isaac McPherson in 1813, in which he stated, "that ideas should freely spread from one to another over the globe, for the moral and mutual instruction of man . . . Inventions then cannot, in nature, be a subject of property. [However] society may give an exclusive right to the profits arising from them, as an encouragement to men to pursue ideas which may produce utility."

Thomas Jefferson believed that the government had a major responsibility for protecting from theft our intellectual property assets; assets important to the Nation's security interests. That view is especially relevant today. U.S. policymakers have stated that our nation's economic integrity is synonymous with our national security. During testimony before the Senate Foreign Relations Committee, November 4, 1993, Secretary of State Warren Christopher said, "in the post-cold war world our national security is inseparable from our economic security." In July 1994, President Clinton's "national security strategy of engagement and enlargement" was published. This document elaborates a new strategy for this new era, and identifies as a central goal "to bolster America's economic revitalization." Safeguarding proprietary economic information and technology is a national priority and an important part of our nation's tradition.

In today's environment, proprietary intellectual property and economic information in the global and domestic marketplace have become the most valuable and sought after commodity by all advanced nations. Within this evolving global environment in which information is created and shared instantaneously over national and global information highways—an environment in which technology is critical to all types of industry—both the opportunities and motives for engaging in economic espionage are increasing.

Some foreign governments, through a variety of means, actively target U.S. persons, firms, industries and the U.S. Government itself, to steal outright critical technologies, data, and proprietary information in order to provide their own industrial sectors not only a competitive advantage but, in fact, an unfair advantage. Similarly, theft or misappropriation of proprietary economic information by domestic thieves is equally damaging.

Foreign intelligence operations directed against U.S. economic interests are neither unusual nor unprecedented. The United States and other major industrial countries have been the targets of economic espionage for decades. However, U.S. Counterintelligence has traditionally been directed at military, ideological or subversive threats to national security. This was due in large part to cold war security concerns, as well as by the reality of U.S. economic and technical predominance.

The end of the cold war has brought with it several changes that have raised the profile of economic espionage. First, the collapse of Soviet communism has caused many foreign intelligence services to reassess collection priorities and redirect resources previously concentrated on cold war adversaries toward economic and technological targets. Second, military and ideological allies during the cold war have become serious economic competitors. The former head of a foreign intelligence service stated on January 9, 1996, that In his country "the State is not just responsible for law making, it is in business as well." He added "it is true that for decades the State regulated the markets to some extent with its left hand while its right hand used the secret services to procure information for its own firms." Third, the globalization of the economy has brought about an environment in which national security and power are no longer measured exclusively by the number of tanks and nuclear weapons but increasingly in terms of economic and industrial capabilities.

And finally, this information age environment challenges existing laws and programs which historically were designed to protect property and invention. Traditional Federal statutes, such as the interstate transportation of stolen property were enacted long before there were computers, fax machines, modems and the other technologies that allows information—valuable information—to be sent instantaneously to anywhere in the world. Now formulas, ideas or proprietary economic information can be stolen with a few keystrokes and under many circumstances no criminal law can be applied to prosecute the offenders.

Obviously, this new era presents a new set of threats to our national security, and presents challenges to existing security, counterintelligence, and law enforcement structures and missions. Despite the challenges, these institutions continue to have as their fundamental duty and purpose as guaranteed in the preamble to the constitution, "to provide for the common defense, promote the general welfare, and secure the blessings of liberty to ourselves and our posterity."

Accordingly, it is our government's responsibility: (1) to take stock as to the resources important to our nation's welfare, liberties and security, that is, the imagination, innovation, and invention, especially in high-technology areas, of our nation's citizens and business institutions, (2) to identify threats to those resources, and (3) to effect provisions for deterring, counteracting, and punishing those who attack or steal those resources.

The Federal Bureau of Investigation has already taken steps to deal with economic espionage. In 1994, I initiated an Economic Counterintelligence Program with a mission to detect and counteract economic espionage activities directed against U.S. interests. Through this program, the FBI has brought to bear both its foreign counterintelligence and criminal investigative jurisdictions, expertise and investigative resources to address this important national security issue. During the past year, the FBI has developed significant information on the foreign economic espionage threat, to include: (1) the identification of actors—the perpetrators of economic espionage; (2) the economic targets of their spying and criminal activities, and (3) the methods used to steal clandestinely and illicitly proprietary economic information and technology.

FBI investigations reveal that numerous foreign powers are responsible for directing, controlling and/or financing economic espionage activities directed against both the government as well as the private sector. Of the approximately 800 economic espionage matters currently being investigated by the FBI, 23 foreign powers are directly implicated.

The targets of economic espionage are varied. Advanced technologies, defense-related industries and critical business information remain the primary targets of the foreign economic espionage activities. In many instances, the industries are of strategic interest to the United States for several reasons: some of them produce classified products for the government; others produce dual-use technology applicable to both the public and private sectors; and others develop leading-edge technologies that are critical to maintaining U.S. Economic security.

These pieces of economic and technological information seldom exist in a vacuum. Foreign countries collect sensitive economic intelligence frequently to enhance both their military capabilities and their economic stability and competitiveness. Likewise, the line separating purely economic intelligence from political intelligence is as difficult to draw as that between technical and military intelligence. At times, foreign policymakers may be interested in our government's economic policy decisions or proprietary information on a U.S. Company's financial stability for political as well as economic reasons.

Neither the FBI nor the U.S. Intelligence Community as a whole has systematically evaluated the costs of economic espionage. A variety of U.S. private sector surveys have attempted to quantify the potential damage in dollar terms, with varying results and a wide spectrum of estimates:

- The U.S. International Trade Commission (ITC) estimated in 1982 that in five selected industrial sectors, piracy of U.S. Intellectual property rights cost the nation's business $6 billion to $8 billion in annual sales and cost U.S. citizens 131,000 jobs.
- In 1987, ITC estimated worldwide losses to all U.S. industries were $23.8 billion. (Using the 1982 average loss ratio of $7 billion = 130,000 jobs, this would constitute a loss of about 450,000 U.S. Jobs.)
- The last study conducted in 1988 by the U.S. ITC, estimated that U.S. companies lost from $43 billion to $61 billion in 1986 alone from foreign intellectual property right infringement.
- In 1992, the American Society for Industrial Security surveyed 246 companies and found that proprietary information theft has risen 260 percent since 1985. The survey Indicated that customer lists are the most frequently stolen category

of U.S. proprietary Information. The survey found that all types of commercial espionage during 1991–92 resulted In major losses to U.S. Firms in the following areas: pricing data ($1 billion), product development and specification data ($597 million), and manufacturing process information ($110 million)—total of $1.2 billion lost.

- In a special report entitled "Trends in Intellectual Property Loss" sponsored by the American Society for Industrial Security (ASIS) co-authored by Richard J. Heffernan and Dan Swartwood, 325 U.S. corporations responded to a double-blind survey—the third in a series. For 1995, 700 incidents of proprietary loss were cited by respondents which reflected a 323 percent increase in this activity between 1992 (9.9 incidents per month) and 1995 (32 incidents per month). Of these incidents, 59 percent were attributable to employees or ex-employees. Fifteen percent were attributable to those with a contractual relationship with the company. In all, 74 percent of the incidents were committed by those who were in a position of trust with the company. In 21 percent of the incidents, foreign involvement was identified. The loss claimed for the 700 incidents was $5.1 billion, approximately 9 percent of the U.S. GNP.

These survey estimates clearly indicate that the actual and potential losses incurred are immense.

In the past, although the FBI has not specifically focused resources on the issue of economic espionage, a sample of ten such investigations, spanning 20 years, reflect the following: value of contracts targeted—$2,100,000,000; potential economic loss prevented—$2,755,740,000; civil damages awarded—$67,000,000.

Despite not having a single definitive dollar loss figure, there are other tangible losses caused by economic espionage. When proprietary economic information is stolen from American companies: Americans lose jobs; U.S. Capital and migrate overseas; and the incentive for research and development investment declines.

Understandably, U.S. industry is reluctant to publicize occurrences of foreign economic espionage. Such publicity can adversely affect stock values, customers' confidence, and ultimately competitiveness and market share. Therefore, gathering the empirical data to quantify the damage is problematic. But regardless of the exact number, the damage caused by economic espionage is significant.

Practitioners of economic espionage seldom use one method of collection in isolation. Instead they conduct coordinated collection programs which combine both legal and illegal, traditional and more innovative methods. FBI investigations have identified various methods utilized by those engaged In economic espionage. Spotting, assessing and recruiting individuals with access to a targeted technology or information is a classical, time proven technique which is well practiced.

As with classical espionage, foreign collectors assess the vulnerabilities of the individual, looking for any personal weaknesses or commonality between them and the targeted person that can be exploited to convince the individual to cooperate.

Other methods include tasking students who come to study in the United States; exploiting non-government affiliated organizations such as friendship societies, international exchange organizations, or import-export companies; hiring away knowledgeable employees of competing U.S. firms with the specific goal of exploiting their inside knowledge; and manipulating legitimate technology sharing agreements so that they also become conduits for receiving proprietary information, to list just a few.

The FBI and other U.S. Government agencies have developed information clearly establishing that economic espionage is a very real and significant problem. However, current statutory remedies do not allow us to counter or to deter effectively this damaging activity. Since the criminal nature of unlawfully taking or appropriating trade secrets or proprietary economic information involves stealing, the most relevant current Federal statute is T18 USC 2314, Interstate Transportation of Stolen Property. Ironically, and indicative of our problem however, this statute was enacted long before computers, copy machines, and instant communication even existed. Indeed, Congress passed this law when it became commonplace to transport stolen property across State lines in automobiles. Unfortunately, some courts have held that intangible proprietary economic information does not qualify as the "goods, wares, merchandise, securities or moneys" set forth in the statute. For example, U.S. espionage statutes, designed to meet the demands of the cold war, do not cover many current economic intelligence-gathering operations because often the information stolen, while sensitive or proprietary, is not classified national defense information. Federal criminal statutes relating to the theft of property often are not applicable because the stolen item is not tangible. Many States have laws against the theft of trade secrets, but these statutes do not apply or are greatly weakened when activity occurs in multiple State jurisdictions. Current Federal and State statutes do not contain a uniform legal definition for intellectual property or technical

information and thus have proven to be inadequate in addressing economic espionage.

Even basic concepts can prove problematic. For example, if an individual downloads computer program codes without permission of the owner, has a theft occurred even though the true owner never lost possession of the original? Similarly, if a U.S. company licenses a foreign company located in a foreign country to use its proprietary economic information, and an employee of the foreign company makes and sells an unauthorized copy of the information to agents of a third country, has any U.S. crime been committed?

Another difficulty with existing law is that it fails to afford explicit protection to the confidential nature of the information in question during enforcement proceedings. By its nature, proprietary economic information derives value from its exclusivity and confidentiality. If either is compromised during legal proceedings, the value of the information is diminished even though the goal of the legal process was to protect the information. Rather than risk such compromise, many companies opt to forego legal remedies in the hope or expectation that the information's residual value will exceed the damage done by a wrongdoer.

Since no Federal statute directly addresses economic espionage or the protection of proprietary economic information in a thorough, systematic manner, the FBI has experienced difficulties prosecuting cases of economic espionage. In several instances, the FBI has conducted investigations where a review of the facts of the case did not fit existing laws and as such the Department of Justice or U.S. Attorney's offices declined prosecution.

In the absence of a modern Federal statute designed to protect U.S. proprietary economic information in a systematic, direct manner, widely divergent outcomes are often produced by current laws, which were designed to counteract other problems. Such inconsistent legal results seriously dilute the deterrent effect of these difficult prosecutions. Let me cite two such examples: in one case, an FBI undercover agent posing as a high-tech buyer agreed to buy a drug fermentation process for $1.5 million from employees of two American biotechnology companies, Schering-Plough and Merck. The defendants agreed to sell a second such process to the undercover agent for six to eight million dollars. Over 750 million dollars in research and development cost had gone into developing the two fermentation processes. The exchange took place and the subjects were immediately arrested and the assets provided were recovered.

As no Federal statute exists which directly addresses the theft of trade secrets, this investigation was pursued as a fraud matter. Each subject was convicted on 12 counts relating to conspiracy, fraud by wire, interstate transportation of stolen property and mail fraud violations. The U.S. District court judge who presided over the trial stated that the subjects attempted to compromise years and years of research undertaken by the victim companies. The Judge added that there are few crimes with regard to monetary theft that could reach this magnitude and sentenced the offenders accordingly.

In contrast, in another 1993 case the FBI arrested two individuals who sold proprietary bid and pricing data regarding the Tomahawk cruise missile program to an FBI undercover agent for $50,000. The U.S. Navy was to award this $3 billion contract to a sole vendor, either Hughes Aircraft or McDonnell-Douglas missile systems. Both companies conceded that the loss of the highly competitive contract would have closed down their missile facilities. Both defendants were convicted of Federal fraud violations. Not withstanding the gravity of the offense, one of the individuals was placed on probation for 1 year and ordered to participate in the home detention program for 60 days. The other was sentenced to 4 months in prison, with credit for time served, and 4 months of home detention.

These and other problems underscore the importance of developing a systemic approach to the problem of economic espionage. Only by adoption of a national statutory scheme to protect U.S. proprietary economic information can we hope to maintain our industrial and economic edge, and thus safeguard our national security.

The FBI supports a two-tiered approach to the problem. First, we advocate dealing specifically with economic espionage and protecting proprietary economic information. Federal law must provide key definitions, punish all manner of wrongful conduct associated with stealing proprietary economic information, provide for extraterritoriality under certain circumstances, preserve existing State law on the subject, and specifically preserve the confidentiality of the information in question during enforcement proceedings. Second, we support amending existing criminal statutes to reinforce and enhance enforcement efforts. We must find solutions to the many impediments that U.S. counterintelligence and law enforcement have experienced when attempting to counter economic espionage.

By doing this, we will recognize that the protection of proprietary economic information and the prevention of economic espionage is both a counterintelligence and law enforcement problem. We should not focus on one to the exclusion of the other but seek, instead, to forge a unified approach to combat a sophisticated threat to U.S. National Interest. The FBI supports such an approach and hopes to see Federal legislation enacted to better protect U.S. national security.

[Note: Attached are additional cases that can be used to supplement the points made in the statement.]

United States General Accounting Office

GAO

Testimony

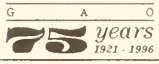
Before the Select Committee on Intelligence
United States Senate

For Release on Delivery
Expected at
10:30 a.m., EST
Wednesday,
February 28, 1996

ECONOMIC ESPIONAGE

Information on Threat From U.S. Allies

Statement for the Record by David E. Cooper, Associate Director, Defense Acquisitions Issues, National Security and International Affairs Division



GAO/T-NSIAD-96-114

Mr. Chairman and Members of the Committee:

I am pleased to be able to provide this statement for the record. We recently completed a report on security arrangements used to protect sensitive information when foreign-owned U.S. companies work on classified Department of Defense contracts.[1] As part of this effort, we examined the threat of foreign espionage facing U.S. defense companies, a concern of today's hearing.

In brief, Mr. Chairman, we reported that, according to the Federal Bureau of Investigation and intelligence agencies, some close U.S. allies actively seek to obtain classified and technical information from the United States through unauthorized means. These agencies have determined that foreign intelligence activities directed at U.S. critical technologies pose a significant threat to national security.

Economic Espionage Efforts of Allies

U.S. intelligence agencies report a continuing economic espionage threat from certain U.S. allies. Our report discussed the espionage activities of five allies.

A goal common to most of these countries was the support of the country's defense industry. Countries seek U.S. defense technologies to incorporate into domestically produced systems. By obtaining the technology from the United States, a country can have cutting-edge weapon systems without the cost of research and development. The cutting-edge technologies not only provide superior weapon systems for a country's own use, but also make these products more marketable for exports.

Country A

According to a U.S. intelligence agency, the government of Country A conducts the most aggressive espionage operation against the United States of any U.S. ally. Classified military information and sensitive military technologies are high-priority targets for the intelligence agencies of this country. Country A seeks this information for three reasons: (1) to help the technological development of its own defense industrial base, (2) to sell or trade the information with other countries for economic reasons, and (3) to sell or trade the information with other countries to develop political alliances and alternative sources of arms. According to a

[1]Defense Industrial Security: Weaknesses in U.S. Security Arrangements With Foreign-Owned Defense Contractors (GAO/NSIAD-96-64, Feb. 20, 1996)

classified 1994 report produced by a U.S. government interagency working group on U.S. critical technology companies,[2] Country A routinely resorts to state-sponsored espionage using covert collection techniques to obtain sensitive U.S. economic information and technology. Agents of Country A collect a variety of classified and proprietary information through observation, elicitation, and theft.

The following are intelligence agency examples of Country A information collection efforts:

- An espionage operation run by the intelligence organization responsible for collecting scientific and technological information for Country A paid a U.S. government employee to obtain U.S. classified military intelligence documents.
- Several citizens of Country A were caught in the United States stealing sensitive technology used in manufacturing artillery gun tubes.
- Agents of Country A allegedly stole design plans for a classified reconnaissance system from a U.S. company and gave them to a defense contractor from Country A.
- A company from Country A is suspected of surreptitiously monitoring a DOD telecommunications system to obtain classified information for Country A intelligence.
- Citizens of Country A were investigated for allegations of passing advanced aerospace design technology to unauthorized scientists and researchers.
- Country A is suspected of targeting U.S. avionics, missile telemetry and testing data, and aircraft communication systems for intelligence operations.
- It has been determined that Country A targeted specialized software that is used to store data in friendly aircraft warning systems.
- Country A has targeted information on advanced materials and coatings for collection. A Country A government agency allegedly obtained information regarding a chemical finish used on missile reentry vehicles from a U.S. person.

Country B

According to intelligence agencies, in the 1960s, the government of Country B began an aggressive and massive espionage effort against the United States. The 1994 interagency report on U.S. critical technology companies pointed out that recent international developments have

[2]Report on U.S. Critical Technology Companies. Report to Congress on Foreign Acquisition of and Espionage Activities Against U.S. Critical Technology Companies (1994)

increased foreign intelligence collection efforts against U.S. economic interests. The lessening of East-West tensions in the late 1980s and early 1990s enabled Country B intelligence services to allocate greater resources to collect sensitive U.S. economic information and technology.

Methods used by Country B are updated versions of classic Cold War recruitment and technical operations. The Country B government organization that conducts these activities does not target U.S. national defense information such as war plans, but rather seeks U.S. technology. The motivation for these activities is the health of Country B's defense industrial base. Country B considers it vital to its national security to be self-sufficient in manufacturing arms. Since domestic consumption will not support its defense industries, Country B must export arms. Country B seeks U.S. defense technologies to incorporate into domestically produced systems. By stealing the technology from the United States, Country B can have cutting-edge weapon systems without the cost of research and development. The cutting-edge technologies not only provide superior weapon systems for Country B's own use, but also make these products more marketable for exports. It is believed that Country B espionage efforts against the U.S. defense industries will continue and may increase. Country B needs the cutting-edge technologies to compete with U.S. systems in the international arms market.

The following are intelligence agency examples of Country B information collection efforts:

- In the late 1980s, Country B's intelligence agency recruited agents at the European offices of three U.S. computer and electronics firms. The agents apparently were stealing unusually sensitive technical information for a struggling Country B company. This Country B company also owns a U.S. company performing classified contracts for DOD.
- Country B companies and government officials have been investigated for suspected efforts to acquire advanced abrasive technology and stealth-related coatings.
- Country B representatives have been investigated for targeting software that performs high-speed, real-time computational analysis that can be used in a missile attack system.
- Information was obtained that Country B targeted a number of U.S. defense companies and their missile and satellite technologies for espionage efforts. Companies of Country B have made efforts, some successful, to acquire targeted companies.

Country C

The motivation for Country C industrial espionage against the United States is much like that of Country B: Country C wants cutting-edge technologies to incorporate into weapon systems it produces. The technology would give Country C armed forces a quality weapon and would increase the weapon's export market potential. The Country C government intelligence organization has assisted Country C industry in obtaining defense technologies, but not as actively as Country B intelligence has for its industry. One example of Country C government assistance occurred in the late 1980s, when a Country C firm wanted to enter Strategic Defense Initiative work. At that time, the Country C intelligence organization assisted this firm in obtaining applicable technology.

Country D

The Country D government has no official foreign intelligence service. Private Country D companies are the intelligence gatherers. They have more of a presence throughout the world than the Country D government. However, according to the 1994 interagency report, the Country D government obtains much of the economic intelligence that Country D private-sector firms operating abroad collect for their own purposes. This occasionally includes classified foreign government documents and corporate proprietary data. Country D employees have been quite successful in developing and exploiting Americans who have access to classified and proprietary information.

The following are examples of information collection efforts of Country D:

- Firms from Country D have been investigated for targeting advanced propulsion technologies, from slush-hydrogen fuel to torpedo target motors, and attempting to export these items through intermediaries and specialty shipping companies in violation of export restrictions.
- Individuals from Country D have been investigated for allegedly passing advanced aerospace design technology to unauthorized scientists and researchers.
- Electronics firms from Country D directed information-gathering efforts at competing U.S. firms in order to increase the market share of Country D in the semiconductor field.

Country E

Intelligence community officials stated that they did not have indications that the intelligence service of Country E has targeted the United States or its defense industry for espionage efforts. However, according to the 1994

interagency report, in 1991 the intelligence service of this country was considering moving toward what it called "semi-overt" collection of foreign economic intelligence. At that time, Country E's intelligence service reportedly planned to increase the number of its senior officers in Washington to improve its semi-overt collection—probably referring to more intense elicitation from government and business contacts.

The main counterintelligence concern cited by one intelligence agency regarding Country E is not that its government may be targeting the United States with espionage efforts, but that any technology that does find its way into Country E will probably be diverted to countries to which the United States would not sell its defense technologies. The defense industry of this country is of particular concern in this regard.

It was reported that information diversions from Country E have serious implications for U.S. national security. Large-scale losses of technology were discovered in the early 1990s. Primary responsibility for industrial security resides in a small staff of the government of Country E. It was reported that this limited staff often loses when its regulatory concerns clash with business interests. The intelligence agency concluded that the additional time needed to eradicate the diversion systems will consequently limit the degree of technological security available for several years. The question suggested by this situation is, if technology from a U.S. defense contractor owned by interests of Country E is transferred to Country E, will this U.S. defense technology then be diverted to countries to which the United States would not sell?

Our report also discusses how the Department of Defense seeks to protect sensitive information and technologies at foreign-owned U.S. companies against such threats. It makes recommendations aimed at improving information security at firms operating under these security arrangements.

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. VISA and MasterCard credit cards are accepted, also. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 6015
Gaithersburg, MD 20884-6015

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000
or by using fax number (301) 258-4066, or TDD (301) 413-0006.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

PRINTED ON RECYCLED PAPER

Statement for the Record

John J. Higgins
Senior Vice President and General Counsel
Hughes Electronics Corporation

Prepared for the United States Senate
Select Committee on Intelligence
and
Committee on the Judiciary,
Subcommittee on Terrorism, Technology
and Government Information

Joint Hearing on Economic Espionage
28 February 1996

INTRODUCTION

Hughes Electronics is a $15 billion corporation primarily involved in the Aerospace and Defense, Telecommunications and Space, and Automotive Electronics industries. These industries are driven by high technology, are highly competitive, and are global in scope. The safeguarding of our intellectual property, which includes our core technologies, our business strategies, our pricing data, etc., is critical to our success and survival in these industries.

Economic espionage, both domestic and foreign, poses a very real threat to Hughes Electronics and, in several cases, has resulted in very real damages. Economic espionage is a matter of significant concern not only to our company's competitiveness, but to the competitiveness of our country in the global marketplace; and it is becoming more and more clear that our national security is directly linked to our economic security. Hughes Electronics commends the Senate Select Committee on Intelligence and the Committee on the Judiciary for their efforts and offers our full support of legislation which addresses the problem of economic espionage.

BACKGROUND

Hughes Electronics has been undergoing substantial change in recent years, much of it directed toward identifying and focusing our resources on the global commercial marketplace. Previously, we were very active selling our military systems to the United States government and its allies and today we continue to do so, but we have now added emphasis on a variety of commercial ventures. Of our approximately $15 billion in annual sales, 60% is derived from commercial endeavors. These include DIRECTV - the 18" satellite dish system, Delco Electronics and their automotive electronics endeavors, Hughes Network Systems - manufacturers of private satellite communication systems, and Hughes Telecommunications and Space - a world leader in commercial communications satellite systems and other such ventures. These commercial businesses are critical to the future of Hughes Electronics.

Just as Hughes has placed emphasis on its success in the global commercial marketplace, countries throughout the world are redirecting their national resources from military to economic programs. Defense industries in the United States, Russia, Europe, Japan and elsewhere are restructuring their technological, engineering, and other resources into new commercial ventures. This strong emphasis of national resources on economic rather than military competition puts business secrets increasingly at risk.

We all realize that the end of the cold war has not brought an end to the foreign intelligence threat, but it has merely changed the nature of that threat. Today it is more diversified and more complex. Many intelligence agencies around the globe are focusing more on targeting economic data and intellectual property identified as having critical value to future growth and development. Right now, it is estimated that at least 50 countries are pursuing economic espionage activities against the United States every day. Unfortunately, many of these countries operate within our borders to steal our information. And many of these are "friendly spies"; nations we count as our allies in other matters.

Unfortunately, the law has not quite kept up with evolving economic dynamics, particularly with respect to law enforcement. Presently, there are no economic espionage counterparts to the military espionage laws. Existing criminal statutes are not clear regarding coverage of intangible intellectual property. Moreover, civil remedies are plagued by the lack of a national standard, the difficulty of proving actual damages, and inaccessibility of international defendants.

As with foreign sponsored economic espionage, domestic economic espionage also poses a critical threat to the economic security of corporations. The same competitive dynamics which entice foreign entities to engage in economic espionage are likewise at work on the domestic front. Intense competition, the huge investments required for research and development, and "make or break" contracts can create the incentive for domestic firms to spy on each other. The impact and damages caused by this domestic espionage can be just as devastating to a corporation as with foreign sponsored espionage.

One such case involving Hughes Electronics was discussed by Louis Freeh, Director of the Federal Bureau of Investigation, in his prepared statement for this hearing. I will provide only a brief description here since it is discussed by Director Freeh. The case involved two individuals who sold Hughes proprietary bid and pricing data to an undercover FBI agent for $50,000. The bid and pricing data was for the "winner-take-all" competition for the Tomahawk Cruise Missile Program, ultimately valued at $3 billion for the winning corporation. The losing corporation would be faced with closing facilities, laying off many highly qualified and loyal employees, and diminished shareholder value. Both individuals pled guilty to violating the only statutes available to the prosecution. The resulting penalties were extremely lenient considering the potential economic impact on the corporations involved.

As you might also readily surmise, Hughes has been the victim of economic espionage on several other occasions involving foreign interests. I will describe a few examples to demonstrate how real the threat is and how real the damages are.

Cases of International Economic Espionage

Although not an entirely new phenomenon, during the period commencing in mid-1993 through the present, Hughes Electronics encountered an increasing variety of incidents involving evidence of economic espionage. Company investigation into these incidents has identified a pattern of assault on company technology and proprietary information causing a negative impact on the company's competitive position and resources. Investigations coordinated by the company have identified a number of such cases, four of which will be cited as examples, which have caused the company great concern. Targets of the economic espionage included not only critical technology but also strategic planning, marketing forecasts, and pricing data. Needless to say, wrongful disclosure of this information in each of these cases would critically affect the company's competitive position. All of these cases have international espionage overtones.

The following cases are representative of incidents known to the company. The facts set forth as follows comprise a brief overview of the investigations:

1. Unauthorized Dissemination Of Hughes Proprietary Marketing Forecasts

During 1993, an internal investigation determined that a former vice president of marketing for a Hughes business unit had come into unauthorized possession and had distributed at least two editions of the unit's New Business Forecasts. The former vice president, who at that time was operating his own company, provided these forecasts as "calling cards" to ingratiate himself with Hughes' competitors so that they might provide work in his new business venture. The data contained in the new business forecasts comprised critical information which would clearly provide a significant advantage to a competitor.

Our investigation determined that one of the companies to which this former vice president had sent copies of the marketing forecasts was a U.S. corporation which was in turn a subsidiary of a government-owned European corporation. It was subsequently learned that copies of these marketing and new business forecasts were forwarded to the European corporation's home office. Follow-up interviews identified a significant interest by these European employees not only in the Hughes data but also in proprietary technical information belonging to other U.S. companies.

2. Unauthorized Dissemination Of Hughes Proprietary Technology

In March of 1995, a scientist with Hughes was tasked with generating a preliminary systems architecture study dealing with the transmission of a satellite television signal to earth. The study was a follow-on to the sale of a commercial satellite to a Southeast Asian customer and was to be part of a proposal and bid package to be submitted by Hughes. Hughes was interested in doing additional business with the customer by handling transmission of the satellite television signal.

The Hughes employee assigned to this task was a twenty year employee who was within six months of eligibility for retirement. In his dealing with the customer, the scientist provided the most complete written compilation of this technology in existence. The description far exceeded the requirements of the systems architecture study.

The scientist ultimately gave up lucrative retirement benefits with Hughes and accepted a position with the customer at a salary estimated at three to four times above what he was earning at Hughes. The customer then declined the Hughes proposal for involvement in the satellite signal transmission, noting they intended to take this task up themselves. They are now in possession of sufficient technological information to accomplish this on their own. Once hired, the Hughes scientist convinced several other key employees to join him in this venture.

3. Hughes Electric Vehicle Technology

In August of 1994 a new U.S. company, funded by a Southeast Asian company, hired the engineering director and two key members of the technical staff from Hughes in an apparent effort to compete for electric car technology. The engineering director was a twenty-two year employee of Hughes. Three key Hughes employees resigned on the same day without providing any reason for their departure. Within a short period of time, five other key Hughes employees were hired by the new company with pay raises approximating 40%.

The transition of employees from Hughes to the new foreign-owned U.S. company, in addition to being a technology drain on the resources of Hughes, provided the new company with all of the essential personnel to compete technologically with Hughes. Additionally, during April of 1995, a package of documents was found in the Hughes mail room containing newly revised and detailed schematics of electric vehicle technology which was about to be sent to the new company.

4. Oil And Gas Refinery Operations Simulator

During September of 1995, in connection with a local homicide investigation in Houston, Texas, several cartons of documents containing Hughes proprietary information were found in the possession of associates of a Hughes employee who was the principal suspect in the homicide.

An investigation determined that this six year engineering employee was apparently given unauthorized access to Hughes proprietary data through an associate who was retiring. The employee entered the facility at night and on weekends and copied an entire project dealing with development of an oil and gas operations simulator and removed the documents from the facility. The Hughes employee, through an associate and with the assistance of a co-worker, began efforts to market the oil and gas refinery simulator in a north African country.

SUMMARY

The above cases are merely examples of Hughes' experiences and only represent the tip of an iceberg of intellectual property theft. Although Hughes responded to each of these incidents, clearly the presence of the proposed legislation would have upped the ante against the U.S. and foreign players involved.

What is perhaps most noteworthy is that the targeted technologies mentioned represent the culmination of many years of prior effort in the defense area and the hard-won but successful application of defense technologies to commercial pursuits. It would indeed be tragic if we did not provide our national law enforcement community the needed tools to assist industry in combating these problems. In many cases U.S. industries are not able to effectively address these matters in foreign and U.S. jurisdictions due to the limitations of civil laws and inability to reach individual or national defendants.

In responding to the heightened need to protect our intellectual property from unauthorized disclosures, Hughes Electronics has developed the "Information Resources Protection (IRP)" program. The program is intended to provide a road map of information for employees to use in their everyday work, both domestically and overseas. The program establishes a management policy, and supporting guidance materials, to identify protection requirements for company information. While there is much more to IRP, many traditional means of protection are prescribed such as locking up documents, and marking and tracking the flow of documents. We believe that these internal measures, along with aggressive use of civil procedures, will provide some help in the fight against economic espionage. Nevertheless, a statutory, criminal deterrent with commensurate punitive provisions is critical to supporting these private responses.

We are committed to providing our support to the Congress as you prepare legislation that will make theft of proprietary information a federal crime within the FBI's investigative jurisdiction. This is absolutely essential in an area of critical national importance that for too long has been considered a state or local matter and not given the stature as a federal crime which theft of tangible property and military technology has historically been accorded. It is also clear that civil litigation, although it has its role, needs to be supplemented by our national justice system in this instance.

In summary, our proprietary information is the intellectual currency we need to redeem our future. We must do everything possible to stem its loss. This legislation is a critical part of that process.

TESTIMONY OF

NORMAN R. AUGUSTINE
PRESIDENT AND CHIEF EXECUTIVE OFFICER
LOCKHEED MARTIN CORPORATION

Before the

Senate Select Committee on Intelligence

Concerning

The Role of the U.S. Intelligence Community
in Promoting U.S. Competitiveness

February 28, 1996

Mr. Chairman and Members of the Committee, I want to thank you for the opportunity to submit this statement on the role of the U.S. intelligence community in promoting U.S. competitiveness.

I do have some strong views on this subject, based upon my experience at Lockheed Martin, which like many U.S. companies is working to expand its markets both at home and abroad, and based upon my previous experience in the public sector and in the private sector at several other companies. Our company has approximately 25,000 employees in the U.S. whose jobs depend upon our ability to sell our products abroad -- and to do so in an ethical and legal fashion against global competitors.

Main Points

The main points that I would like to make today are these:

I believe the U.S. intelligence community can make an enormous contribution to the conduct of global trade and U.S. competitiveness **by helping assure that generally accepted principles of fairness are in fact practiced by others in the marketplace**; that is, to protect U.S. firms from exploitation by firms or agencies of other nations which may choose to disregard generally accepted practices concerning, for example, payments to agents. It is in this area of counterintelligence where I believe the greatest contribution may be made and where our companies have little or no ability to help themselves.

Furthermore, I believe that **the U.S. intelligence community does have an important role in improving U.S. competitiveness by preventing foreign espionage**, whether on U.S. soil or in U.S.-based companies' offices and facilities around the world. In so doing, U.S. intelligence agencies should rely on overt, not covert, techniques, helping U.S. companies improve their ability to safeguard proprietary information. Some policymakers and even some aerospace executives have suggested that it may be appropriate for U.S. intelligence agencies to engage in economic espionage on behalf of U.S. companies. One of my colleagues has gone so far as to suggest, "If we're willing to do dirty tricks for the defense part of national security, then why aren't we able to do dirty tricks for the economic part?" My belief is that U.S. intelligence agencies should not become involved in covert operations in the economic realm other than to ferret out wrong-doing by others.

Others may argue that there exists a new de facto world order in which many governments will be conducting economic espionage -- and that the Cold War has now been replaced with a life-or-death economic war. Indeed, some intelligence analysts suggest that state espionage agencies are now more motivated than they were during the Cold War, because they are working to advance their own country's interests rather than that of some broad strategic alliance.

I am well aware that there is evidence that other countries, even allies, have no qualms about conducting this type of activity. A growing number of nations have become very active in gathering intelligence on specific industries and companies and sharing that information with their domestic industries. Typically, these nations have infrastructures that easily internalize high-technology information and use it in competition against U.S. firms. This is facilitated in those countries that have single, often government-owned, "national champion" firms operating in such areas as defense, for example.

Aerospace and defense companies hold a special attraction for espionage agencies, since the information to be garnered from such companies would include proprietary data as well as information vital to national security. A recent survey of U.S. companies by a Connecticut consulting group reported that a solid 100 percent of aerospace companies believe that a competitor – either domestic or international -- has used intelligence techniques against them.

During 1994, 74 U.S. companies reported 446 incidents of suspected targeting be foreign governments, either domestically or overseas. Lockheed Martin has not been immune. In the last few months, for example, an overseas office of our company was burglarized in what clearly

was an incident of industrial espionage. Objects with obvious "street value" such as computers and other electronic equipment were ignored, while files including program, legal and financial data, as well as customer contact information, were taken. We reported the incident to U.S. Government agencies, as well as local authorities. This incident serves as a valuable reminder that we must remain vigilant against those who seek to misappropriate sensitive or proprietary information for competitive gain.

However, I feel that **it is entirely inappropriate for government agencies to assist corporations to engage in unfair trade practices**. This has been the consistent trade negotiation position of the United States, and I can see no reason to turn our back now on principles of free and fair trade. In a similar vein, simply because others may on occasion bribe foreign officials does not provide a justification for U.S. firms to resort to such behavior. The same logic applies to the matter of industrial espionage.

Finally, U.S. intelligence agencies **possess a considerable amount of raw economic and technical information as well as analytic capabilities that could be broadly useful to U.S. companies** attempting to penetrate markets overseas. While it's true that the intelligence community has focused historically on collecting and analyzing information relevant to military and political affairs, even this information could be a help to some U.S. companies. And a broader array of more fundamental information derived from public sources on the technological capabilities of foreign competitors and the like could be a help to a wider set of U.S. companies.

Let me add that facilitating timely access to this material and to the similar information and analyses collected by other federal agencies, is equally important. To address this problem, I

would recommend that Congress consider expanding the mandates of the National Technology Transfer Center and the National Information (fiber optic) Highway, so that they can permit access not only to technologies from federally-sponsored research projects that have commercial applications, but also to this competitively valuable data on foreign markets collected by federal agencies. More details about this proposal appear below.

Overview of the Problem

There is a widespread recognition that American corporations in a broad range of industries are gradually losing their pre-eminent positions in global commerce. This phenomenon is commonly referred to as a decline in U.S. competitiveness. The point that I would emphasize is that this apparent decline is the result of a complex set of factors.

Some of these factors, like the reconstruction of Europe and Japan following the devastation of war, are to be expected -- indeed, welcome. In fact, our nation deserves much credit for helping bring this about. Some factors are within our own control -- we need to strengthen our educational system, improve the infrastructures that support productive activity in the U.S., and work harder, frankly, to produce quality products that foreign as well as domestic consumers want to buy.

A non-public GAO report presented a few years ago to the House Judiciary Committee concluded that economic espionage represents a serious threat to U.S. economic interests. Foreign officials who have directed the commercial infiltration of U.S. businesses have defended their actions as an essential and cost effective way for their countries to keep abreast of international commerce and technology. But the impact on the U.S. is unacceptable. There is

little information available about the exact costs of economic espionage because many American corporations avoid discussing the extent to which they have been hurt by it. However, the IBM Corporation alone estimates that its own losses have been in the billions. Many other firms are simply unaware of the extent of such activity, being of the school that "there is no evidence of the enemy ever having successfully used camouflage against us."

There are two especially salient points to make about potential losses due to economic espionage. First, several former Directors of the Central Intelligence Agency have pointed out that economic espionage is a particular concern with nations in which there is either state ownership of businesses, or an extremely close cooperative relationship between industries and the state. Obviously, when there is no clear separation between businesses and government agencies, the likelihood increases that the intelligence agency of a government would view the economic success of the businesses as part of its official mission. This exacerbates an already difficult situation which exists when U.S. companies are forced to compete against foreign governments -- with the latter's power to pass laws, print money and exercise political influence.

Second, the incidence of foreign economic espionage that targets the defense industry and defense-related critical technologies raises particular concerns because of its national security implications. In one example, the former head of a foreign intelligence agency alleged that a company owned by that foreign government was able to win a billion-dollar contract to supply fighter jets to India through its use of information provided by the intelligence service about the competing bids from two U.S. companies. Undoubtedly, this type of unethical behavior, if true, has a negative impact for American business because of the loss of potential contracts. But the

long-term damage to the global competitiveness of U.S. firms, and ultimately to the integrity of the defense industry and our national security, is cause for even more serious concern.

One vital part of our infrastructure, the part we are discussing today, is our base of information and understanding about foreign markets. What companies participate in those markets? Who is poised to enter? With what products? What products are in the pipeline? What foreign laws and regulatory schemes apply? Are there opportunities for sales to foreign government agencies? What special procurement rules apply? What resources and support are available to U.S. companies considering a leap into a new market? What technological breakthroughs have been achieved abroad? U.S. companies of all sizes in all industries obviously need access to reliable information of this type which can be derived from publicly available sources in order to make reasoned decisions about what foreign markets they should attempt to enter -- or not enter.

To varying degrees, this information is collected by private corporations themselves. We at Lockheed Martin certainly make an effort to understand our foreign competition and foreign markets -- and when we are not competing against foreign governments, we have met with good success. For example, we feel we are particularly good at assessing the technical performance capabilities of products that have already been placed in the open market by our competitors. But our knowledge about foreign markets falls short of what would be ideal, however, even though we are a sizable company. Our understanding about foreign markets is uneven -- we know more about trends and opportunities in some geographic areas than others -- and we wish we knew more about emerging technologies, before they show up in competing products. And we collect

and analyze information about foreign markets only at great cost and with great duplication of similar efforts by other U.S. firms.

Each company's needs will be different, obviously, although we can assume that smaller companies and those just starting to market their products abroad will be the ones with the most to gain from some kind of organized effort to collect data about foreign markets.

The U.S. intelligence community and other federal agencies are already involved in collecting a great deal of valuable public information about foreign markets. Often, however, this information is not compiled on a timely basis, not adequately indexed, lacks an "industrial" perspective, and in many instances is only housed in U.S. embassies abroad or vaults at home. The CIA has a valuable ongoing operation called the Foreign Broadcast Information Service, or FBIS, that regularly translates and indexes newspaper publications and radio broadcasts from over 100 countries around the world. Although this information is available through government depository libraries on microfiche, it is not easily accessible to private companies, and certainly not on a timely basis.

I mentioned that the comparative decline in U.S. competitiveness may be traced to some degree to economic espionage encouraged or even sponsored by foreign governments. Increasingly, we measure national power and national security in economic as well as military terms. We also measure quality of life at least in part in terms of America's competitiveness. The position of the U.S. on the cutting edge of technological innovation makes us a primary target for technology theft. The trend of state-sponsored espionage that targets the business decisions and technologies of U.S. corporations apparently has become more widespread in the

last decade, but it could potentially become the predominant form of foreign espionage as we move away from the Cold War era. Since 1989, the intelligence community has been focusing on the economic espionage issue, and the directors of the FBI and CIA have both indicated that they expect the recent upward trend to continue.

As Alvin Toffler stated in his recent book, *Powershift*, "Spying, to a greater extent than at any time in the past century, will be pressed into service in support not only of government objectives but of corporate strategy as well, on the assumption that corporate power will necessarily contribute to national power." Three years ago, when I testified on this same topic, I quoted a former House Committee Chairman, who said that the testimony presented to his Committee "painted a dark and sinister picture of how foreign economic espionage activities by countries such as France and Japan have cost American companies billions of dollars and have hurt U.S. competitiveness in the global marketplace."

Suggested Responses

In responding to the question of what the intelligence community can and should be doing to improve U.S. competitiveness, I would like to address the competitiveness issue in two parts. First of all, I think there are additional resources and expertise that these agencies can offer U.S. companies to improve their ability to compete internationally. Second, and far more important, I believe that the intelligence agencies have a critical role to play in combating economic espionage and illegal/unethical business practices such as the payment of bribes ... a role wherein U.S. industry can do relatively little to protect itself.

As I mentioned, I have a specific suggestion for how to expand the role of the U.S. intelligence community in making U.S. companies more competitive internationally. I would recommend that Congress consider asking both the U.S. intelligence agencies and other agencies of the federal government to contribute whatever in-the-clear information and analyses they have about individual foreign companies, their products, foreign industries, foreign regulatory regimes, and foreign markets to a unified national information database where it can be accessed more readily by U.S.-based companies. This would include the translation of selected publicly-available technical reports.

While much of the present focus of U.S. intelligence agencies is on military and political affairs, even this information, to the extent it is unclassified, could be of help to some companies, particularly those wishing to sell to foreign governments and those considering particularly large investments. U.S. intelligence agencies and other federal agencies could expand the present scope of their data collection efforts to include industry- and even company-specific information from publicly-available sources.

Congress should consider making this new database accessible through the National Technology Transfer Center in Wheeling, West Virginia. You will recall that Congress created this Center to make federally-sponsored technology research results, such as findings by federal research laboratories, available to American businesses and industries for commercial product development at a single point of access. The Center is intended to facilitate the transfer of government-sponsored technologies to American businesses, in order to improve U.S. competitiveness.

11

Federally-generated information and analysis about foreign markets could be readily added to this database and accessed by U.S. companies. Access to the National Technology Transfer Center itself will be vastly improved by the fiber optic network provided by the High Performance Computing Act enacted by Congress a few years ago. Information about local and regional political events, specific foreign markets, opportunities, and resources available to assist U.S. companies competing abroad, and even the state-sponsored economic espionage activities being practiced by other governments could easily be collected and provided to U.S. companies through this information network and the NTTC. This information should be accessible by all U.S. companies (which may mean that it would have to be accessible to U.S. subsidiaries of foreign companies, as well.)

With regard to the specific problem of economic espionage sponsored by foreign governments and illegal business practices conducted by foreign competitors, I believe the U.S. intelligence community should continue to be involved in counterintelligence efforts. For example, the FBI and CIA already have a policy of notifying targeted U.S. corporations once a government-sponsored infiltration effort has been detected. A few years ago, President Bush issued a national security directive placing increased emphasis on countering foreign economic espionage. While this directive is non-public, I understand that approximately forty percent of it addresses the targeting of American corporations by foreign intelligence agencies.

Unfortunately, it is clear that some of the countries who sponsor economic espionage will not be easily persuaded into ceasing their operations. For example, news reports indicate that the FBI has delivered private protests to the French government objecting to the infiltration of the European offices of certain U.S. companies.

Conclusion

Ultimately, I believe there are selected, important roles that the U.S. intelligence community can undertake to improve U.S. competitiveness and combat the allegedly growing wave of foreign state-sponsored economic espionage and illegal business practices.

The provision of counterintelligence services and foreign open source information would certainly help U.S. firms, but I would also hope that the United States could set a good example for other nations by refraining from using U.S. intelligence agencies unfairly. We should be setting a good example of free and honest commercial relations, and continue to encourage other nations to abide by these same free trade principles. And my final key point: We should, in the same vein, seek to prevent governments from becoming direct competitors in the marketplace and thereby undermining the entire concept of free trade and the free marketplace.

* * * *

U.S. Department of Justice

Federal Bureau of Investigation

Office of the Director

Washington, D.C. 20535

STATEMENT

OF

LOUIS J. FREEH
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

SENATE SELECT COMMITTEE ON INTELLIGENCE

AND

SENATE COMMITTEE ON THE JUDICIARY,
SUBCOMMITTEE ON TERRORISM,
TECHNOLOGY AND GOVERNMENT INFORMATION

HEARING ON
ECONOMIC ESPIONAGE
FEBRUARY 28, 1996

ECONOMIC ESPIONAGE

The development and production of proprietary economic information is an integral part of virtually every aspect of United States trade, commerce and business and, hence, is essential to maintaining the health and competitiveness of critical segments of the United States economy. The theft, misappropriation, and wrongful receipt, transfer, and use of United States proprietary economic information, particularly by foreign governments and their agents and instrumentalities, but also by domestic malefactors, directly threatens the development and production of that information and, hence, directly imperils the health and competitiveness of our economy.

The ever increasing value of proprietary economic information in the global and domestic marketplaces, and the corresponding spread of technology, have combined to significantly increase both the opportunities and motives for conducting economic espionage. As a consequence, foreign governments, through a variety of means, actively target U.S. persons, firms, industries and the U.S. government itself, to steal or wrongfully obtain critical technologies, data, and information in order to provide their own industrial sectors with a competitive advantage. Similarly, theft or misappropriation of proprietary economic information by domestic thieves has also increased.

The resulting security environment presents a new set of threats to our national security, and presents challenges to existing security, intelligence, counterintelligence and law enforcement structures and missions. But in this new era these institutions continue to have the fundamental purpose "to provide for the common defense, promote the general welfare, and secure the blessings of liberty to ourselves and our posterity." This

clause from the preamble of the Constitution bestows a sacred trust to the U.S. government, assigning responsibility for protecting the lives and personal safety of Americans, maintaining our political freedom and independence as a nation and providing for the well-being and prosperity of our nation.

The United States has become increasingly aware of the economic espionage threat to U.S. interests and U.S. policy-makers have begun to equate economic security with U.S. national security. The March 1990 and February 1995 national security strategies published by the White House focus on economic security as an integral part not only of U.S. national interest but also of national security. On November 4, 1993 before the Senate Foreign Relations Committee, Secretary of State Warren Christopher stated, "In the post-Cold War world, our national security is inseparable from our economic security." Secretary Christopher went on to emphasize "the new centrality of economic policy in our foreign policy."

Additionally, in February 1995, President Clinton published "A National Security Strategy of Engagement and Enlargement" which identified as one of our nation's three central strategy goals to bolster America's economic revitalization. Finally, in an October, 1995 issue of FOCUS magazine, Bruce Lehman, Commissioner of Patents and Trademarks, stated, "what America has to sell to the world is its genius, and if we don't get other countries to provide a system that makes a market for that genius and, secondly, do everything we can to set up market forces that encourage our inventors to exploit that market, we are going to have an extremely hobbled economy." Lehman went on to state, "I favor strong intellectual property rights for U.S. investors. Their creations are the wealth of America, and if you don't acknowledge those rights you have no wealth."

Consistent with U.S. national security policy since 1990, the Federal Bureau of Investigation initiated an Economic Counterintelligence program in 1994 with a mission to collect information and engage in activities to detect and counteract foreign power-sponsored or coordinated threats and activities directed against United States' economic interests, especially acts of economic espionage. This program does not involve offensively collecting economic information; it is defensive in nature with the ultimate goal of protecting U.S. national security. This goal has and will continue to be accomplished by the application of investigative tools, techniques and remedies available through the authorities and jurisdictions assigned to both the FBI's Foreign Counterintelligence and Criminal Investigative Programs. Through the Economic Counterintelligence program, the FBI has developed significant information on the foreign economic threat, to include the identification of actors, targets and methods utilized.

ACTORS

Foreign intelligence operations directed against U.S. economic interests are neither unusual nor unprecedented. The United States and other major industrial countries have been the targets of economic espionage for decades. However, counterintelligence, which is the identification, penetration and neutralization of foreign intelligence activities that threaten U.S. national security, has traditionally been directed at military, ideological or subversive threats to national security. This was due in large part to Cold War security concerns, as well as by the reality of U.S. economic and technical predominance.

In today's world, a country's power and stature are often measured by its economic/industrial capability. Therefore, foreign governments, their ministries, such as those dealing with finance and trade, and major industrial sectors are increasingly

expected to play a more prominent role in their respective country's collection efforts. While a military rival steals documents for a state-of-the-art weapon or defense system, an economic competitor steals a U.S. company's proprietary business information or government trade strategies. Just as a foreign country's defense establishment is the main recipient of U.S. defense-related information, foreign companies and commercially oriented government ministries are the main beneficiaries of U.S. economic information.

Foreign governments pose various levels and types of threats to U.S. economic and technological information. Some ideological and military adversaries continue their targeting of U.S. economic and technological information as an extension of a concerted intelligence assault on the United States conducted throughout the Cold War. The end of the Cold War has not resulted in a peace dividend regarding economic espionage. Just recently, one foreign leader urged better utilization of stolen technology to enhance his country's national security. He stated that currently "only 15 to 20 percent" of the information acquired by spies is being used "even though sometimes special services receive the freshest technological advances literally straight off the pages" of foreign blueprints and manuals.

Other governments targeting U.S. economic and technological information are either longtime allies of the United States or have traditionally been neutral. These countries target U.S. economic and technological information despite their friendly relations with the United States. In some cases, they take advantage of their considerable legitimate access to U.S. information and collect sensitive information more easily than our traditional adversaries. In addition, some of the countries traditionally considered allies have infrastructures that allow them to easily internalize high-tech information and utilize it in competition against U.S. firms. On

January 9, 1996, the former head of a foreign intelligence service told a German television station that in his country "the state is not just responsible for law making, it is in business as well." He added that "It is true that for decades the state regulated the markets to some extent with its left hand while its right hand used the secret services to procure information for its own firms."

In general, the governments and companies of highly industrialized nations collect economic intelligence to gain a competitive edge over major economic rivals, either across the board or in specific industries. In addition, intelligence is collected on U.S. Government plans and policies with regard to trade and industry. Other less industrialized countries tend to limit their economic collection activities to a few key industrial sectors. Current FBI investigations reflect 23 countries engaged in economic espionage activities against the United States.

TARGETS

The targets of economic espionage are varied but high-technology and defense-related industries remain the primary targets of foreign economic intelligence collection operations. The industries that have been the targets in most cases of economic espionage and other collection activities include biotechnology; aerospace; telecommunications, including the technology to build the National Information Infrastructure; computer software/hardware; advanced transportation and engine technology; advanced materials and coatings, including "stealth" technologies; energy research; defense and armaments technology; manufacturing processes; and semiconductors. Proprietary business information, i.e., bid, contract, customer and strategy information, in these sectors is aggressively targeted, as well.

Foreign collectors have also shown great interest in government and corporate financial and trade data.

The industries described above are of strategic interest to the United States because they produce classified products for the government, produce dual-use technology used in both the public and private sectors, and are responsible for leading-edge technologies critical to maintaining U.S. economic security. Many other U.S. high-tech industrial sectors have been targeted. Any foreign company competing for a sale or a piece of a market share, regardless of the market, could resort to intelligence activities as a "force multiplier" to improve its chances.

A few recent examples of the targeting activities described above include: a foreign government-controlled corporation targeting U.S. proprietary business documents and information from U.S. telecommunications competitors; the acquisition of technical specifications for a U.S. automotive manufacturer's product by a foreign competitor; the attempted acquisition in violation of U.S. export laws of a U.S. company's radar technology; the targeting and acquisition of several U.S. companies' proprietary biotechnology information; and the theft of a U.S. company's data and technology regarding the manufacture of microprocessors.

Economic intelligence data seldom exist in a vacuum. Collection of sensitive foreign economic intelligence frequently enhances a nation's military, as well as economic capabilities. Likewise, the line separating purely economic intelligence from political intelligence is as difficult to draw as that between technical and military intelligence.

Types of U.S. government economic information, especially pre-publication data, of interest to foreign

governments and intelligence services as determined through FBI investigations include: U.S. economic, trade and financial agreements; U.S. trade developments and policies; U.S. national debt levels; U.S. tax and monetary policies; foreign aid programs and export credits; technology transfer and munitions control regulations; U.S. energy policies and critical materials stockpiles data; U.S. commodity policies; and proposed legislation affecting the profitability of foreign firms operating in the United States.

IMPACT

Costs of economic espionage have not been systematically evaluated by the U.S. Intelligence Community or the FBI. The U.S. private sector, for its part, has only recently begun to estimate its losses to commercial espionage and other economic intelligence operations. To date, the private sector's cost estimates have generally been based upon small, unrepresentative samples of the U.S. business community and have tended to emphasize companies with holdings in the United States rather than overseas. Understandably, U.S. industry is reluctant to publicize occurrences of foreign economic and industrial espionage. Such publicity can adversely affect stock values, customers' confidence, and ultimately competitiveness and market share. Nevertheless, in the last few years, there have been a number of studies and estimates which have attempted to quantify the scope and impact of economic espionage.

- In 1992, a survey by the American Society for Industrial Security found that all types of commercial espionage during 1991-92 resulted in major losses to U.S. firms in the following areas: pricing data ($1 billion), product development and specification data ($597 million), and manufacturing process information ($110 million).

- The January, 1995 issue of "Law and Policy in International Business" stated that the White Houee Office of Science and Technology estimated losses to U.S. businesses from foreign economic espionage at nearly one hundred billion dollars per year.

- The October 1995 issue of "FOCUS" magazine dealt with the loss of U.S. intellectual property and estimated that the unauthorized copying and counterfeiting of medicines by Argentina, Brazil, India and Turkey alone is costing U.S. drug firms more than 1.5 billion dollars annually.

METHODS

Practitioners of economic espionage seldom use one method of collection, rather they have concerted collection programs which combine both legal and illegal, traditional and more innovative methods. Investigations have and continue to identify the various methods utilized by those engaged in economic espionage and to assess the scope of coordinated intelligence efforts against the United States. The following examplee illustrate some of the methods utilized to engage in economic espionage.

An intelligence collector's best source is a trusted person inside a company or organization whom the collector can task to provide proprietary or classified information. These individuals are approached due to their legitimate and direct access to information. In some instances the insider is selected due to their apparent willingness to engage in unlawful or clandestine activity. For example, between 1986 and 1990, Dr. Ronald Hoffman, a rocket scientist and lead researcher for Science Applications International Corporation (SAIC), sold SAIC-developed technology which was restricted for export to four

foreign companies. The technology sold consisted of computer codes developed for the U.S. Air Force to be utilized in Star Wars projects, but had commercial applications available nowhere else in the world. Press reports have stated that these companies, which were said to be years behind U.S. firms in space technology, have since gained a significant competitive advantage in the space industry.

Some foreign governments task foreign students specifically to acquire information on a variety of economic and technical subjects. In some instances, countries recruit students before they come to the United States to study and task them to send any technological information they acquire back to their home country. Additionally, as an alternative to compulsory military service, one foreign government has an organized program to send interns abroad, often with the specific task of collecting foreign business and technological information.

Upon completion of their studies, some foreign students are then encouraged to seek employment with U.S. firms to steal proprietary information. Although similar to clandestine recruitment used traditionally by intelligence services, often no intelligence service is involved, only a competing company or non-intelligence government agency. The collector then passes the information directly to a foreign firm or the government for use in its research and development (R&D) activities.

In 1989, the FBI conducted interviews of individuals who admitted to having been recruitments of a foreign intelligence service. Two of the individuals stated that they were recruited by the intelligence service just prior to their departure to study in the United States. These individuals worked at the behest of the intelligence agency while studying in the United States. Upon completion of their studies, both

obtained positions with U.S. firms and continued their espionage activities, then directed at their employers, on behalf of the intelligence agency. The individuals each operated at the behest of that agency for 20 years.

Other FBI investigations have identified that some foreign governments exploit existing non-government affiliated organizations or create new ones, such as friendship societies, international exchange organizations, import-export companies and other entities that have frequent contact with foreigners, to gather intelligence and to station intelligence collectors. They conceal government involvement in these organizations and present them as purely private entities in order to cover their intelligence operations. These organizations spot and assess potential foreign intelligence recruits with whom they have contact. Such organizations also lobby U.S. government officials to change policies the foreign government considers unfavorable.

Foreign companies typically hire knowledgeable employees of competing U.S. firms to do corresponding work for the foreign firm. At times, they do this specifically to gain inside technical information from the employee and use it against the competing U.S. firm. For example, the FBI has identified an association of consultants, all of whom were long-term employees of a major U.S. corporation, attempting to sell proprietary high technology to a foreign power. These consultants have 1.5 million dollars in contracts with the foreign power and have offered to provide technology and guidance to the country in order to facilitate their development in the area of technology and allow them to compete with the United States. The result is a loss of proprietary information estimated by the U.S. corporation at billions of dollars.

For example, in 1988, a U.S. automotive manufacturer of a military vehicle was contacted by a foreign automotive

manufacturer who requested a limited licensing agreement with the U.S. manufacturer to allow access to technical data on the military vehicle in order to bid on a contract to build similar vehicles for the foreign country. The U.S. manufacturer agreed but notified the foreign manufacturer of the proprietary nature of the information provided. The U.S. manufacturer was subsequently advised that the contract was awarded to a second foreign manufacturer. In 1993, the second foreign manufacturer produced its first prototype vehicle and displayed the vehicle at a major auto show. Except for the engine, the prototype is essentially a copy of the U.S. manufacturer's vehicle. According to the U.S. manufacturer, this prototype was produced too quickly to have been the product of reverse-engineering. It is not clear that any crime was committed here, but it appears that the specifications licensed to the first foreign manufacturer were provided to the second through an illicit means.

FBI investigations have determined that some countries frequently hire well-connected consultants to write reports on topics of interest and to lobby U.S. Government officials on the country's behalf. Often, the consultants are former high-ranking U.S. Government officials who maintain contacts with their former colleagues. They exploit these connections and contract relationships to illegally acquire protected information, and to gain access to other high-level officials who are currently holding positions of authority through whom they attempt to further illegally acquire protected information.

During joint R&D activities, foreign governments routinely request to have an on-site liaison officer to monitor progress and provide guidance. Using their close access to their U.S. counterparts conducting joint R&D, particularly in the defense arena, liaison officers have been caught wrongfully removing documents that are clearly marked as restricted or classified.

In October 1984, Recon Optical, a U.S. defense contractor and manufacturer of surveillance cameras, signed a 4-year, 40 million dollar contract with a foreign Government to design a top-secret airborne surveillance camera system for that governments intelligence service. Terms of the contract allowed three Air Force officers from that country to work in Recon's plant outside of Chicago. However, after months of disagreement and cost disputes, the U.S. company finally stopped the work in May 1986 and dismissed the three officers. As they left, the officers were caught by security guards stealing boxes of documents. Some of the documents described plans to steal Recon's secret and commercially valuable surveillance camera technology. Documents indicated that, throughout the working relationship, the officers had passed technical drawings to the their country's defense company, Electronics-Optics Industries, Ltd., enabling that country to build its own system.

NEED FOR LEGISLATION

As evidenced by the above, foreign powers, through a variety of means, actively target persons, firms and industries in the U.S. and the U.S. Government itself, to steal or wrongfully obtain critical technologies, data, and information in order to provide their own industrial sectors with a competitive advantage. There are gaps and inadequacies in existing federal laws which necessitate a federal statute to specifically proscribe the various acts defined by economic espionage and address the national security aspects of this crime.

Since no Federal statute directly addresses economic espionage or the protection of proprietary economic information in a thorough, systematic manner, investigations and prosecutions attempt to combat the problem by using existing laws, all of which were designed to counteract other problems. The Interstate

Transportation of Stolen Property Act[1] is an example. This law was designed to foil the "roving criminal" whose access to automobiles made movement of stolen property across state lines sufficiently easy that state and local law enforcement officials were often stymied. While the law works well enough for crimes involving traditional "goods, wares, or merchandise," it was drafted at a time when computers, biotechnology, and copy machines didn't even exist. It is, consequently, not particularly well suited to deal with situations in which information alone is wrongfully duplicated and transmitted electronically across domestic and international borders. One court has observed, for example, that "[t]he element of physical 'goods, wares, or merchandise' in §§ 2314 and 2315[2] is critical. The limitation which this places on the reach of the Interstate Transportation of Stolen Property Act is imposed by the statute itself, and must be observed."[3]

Other existing statutes used by law enforcement agencies on a day-to-day basis to combat economic espionage have similar limitations. For example, the Mail Fraud statute[4] may be used only if an economic espionage scheme involves the use of the mail. Similarly, the Fraud by Wire statute[5] requires an intent to defraud as well as the use of wire, radio, or television.

Even basic concepts can prove problematic. For example, if an individual "downloads" computer program code

---

[1] 18 U.S.C. § 2314. (U)

[2] 18 U.S.C. 2315, dealing with the sale or receipt of stolen property. (U)

[3] United States v. Brown, 925 F.2d 1301 (10th Cir. 1991). (U)

[4] 18 U.S.C. § 1341. (U)

[5] 18 U.S.C. § 1343. (U)

without permission of the owner, has a theft occurred even though the true owner never lost possession of the original? Similarly, if a company doing business in the U.S. licenses a foreign company located in a foreign country to use proprietary economic information and an employee of the second makes and sells an unauthorized copy of the information to agents of a third country, has any U.S. crime been committed?

Another difficulty with existing federal law is that it may not afford explicit protection to the confidential nature of the information in question during enforcement proceedings. By its nature, proprietary economic information derives value from its exclusivity and confidentiality. If either or both are compromised during legal proceedings, than the value of the information is diminished notwithstanding that the proceeding was initiated to vindicate that value in the first place. Rather than risk such compromise, an owner may forego vindication of his or her legal rights in the hope or expectation that the information's residual value will exceed the damage done by a wrongdoer.

Over the past several years, the FBI has experienced difficulties prosecuting cases of economic espionage. The FBI has attempted to use various criminal statutes currently in force to counter economic espionage, but these laws do not specifically cover the theft or improper transfer of proprietary information and, therefore, are insufficient to protect these types of items. In several instances, the FBI has conducted investigations only to have prosecutions or permission to use further investigative procedures declined by the Department of Justice or U.S. Attorney's offices because of lack of criminal predicate.

In an investigation mentioned earlier regarding a consultant group engaged in contracts with a foreign power for

the illicit sale of proprietary information from a U.S. corporation, an Assistant U.S. Attorney denied a request for consensual monitoring of a subject. Citing United States v. Brown, in which the Supreme Court ruled that trade secrets did not constitute "goods, wares, merchandise, securities, nor moneys" as required by the Transportation of Stolen Property in Interstate/Foreign Commerce statute, the AUSA decided that the subjects's actions did not constitute criminal behavior but were merely competitive business practicee.

A second FBI investigation in which prosecution was declined involved the previously discussed case in which a U.S. automotive manufacturer entered into a limited licensing agreement with a foreign manufacturer. After a second foreign manufacturer produced a vehicle with many similarities to the U.S. company's product, the U.S. company alleged that the first foreign manufacturer provided the second with the U.S. manufacturer's proprietary information which the second then used in its vehicle. The Department of Justice returned an opinion stating that "case law is clear that [for Federal theft statutes to be invoked] there must be an actual theft of physical property, not an idea or 'information.'" The Department of Justice stated that if the U.S. company could acquire one of the alleged copied vehicles and "reverse-reverse-engineer" it, and if they could find parts in it that contain patented technology, then the U.S. company may have a patent infringement case.

In a third example, the FBI investigated an information broker who was engaged by two foreign companies to gather proprietary bid information from a major U.S. company regarding a multi-million dollar international construction project. The information broker contacted several employees from the U.S. company, paid them for information, and passed the information on to the foreign companies. The information broker was then paid a large sum of money for his services. For lack of a more applicable violation, the case was investigated as a Wire Fraud

violation but a U.S. Attorney's office declined to prosecute the information broker. Significantly, a similar investigation regarding the same construction project and foreign companies was initiated in the United Kingdom. This investigation resulted in prison sentences for two other information brokers headquartered in England.

Two other recent examples demonstrate the widely varying outcomes in cases involving this type of criminal activity. In both of these instances, successful prosecutions occurred but the penalties in one did not effectively deter the activities.

In January, 1990, a source advised the FBI that two individuals sought to sell pharmaceutical trade secrets which had been stolen from the Schering-Plough Company and Merck and Company, Inc. One of the individuals had been a research scientist with the aforementioned companies and the other owned and operated a research laboratory. The pharmaceutical trade secrets involved two fermentation processes which were and are covered by active patents.

In February, 1990, an FBI undercover agent posing as a buyer for the fermentation processes was introduced to the individuals who agreed to sell one of the processes to the undercover agent for 1.5 million dollars; thereafter, the second process would be sold to the undercover agent for six to eight million dollars. The exchange took place in August, 1990, after which the subjects were immediately arrested and the assets provided were recovered.

Personnel with Schering-Plough and Merck and Company advised that over 750 million dollars in research and development cost had been incurred in developing the two fermentation processes. As no Federal statute exists which directly addresses

the theft of trade secrets, this investigation was pursued as a fraud matter. Each subject was indicted on 13 counts related to conspiracy, fraud by wire, interstate transportation of stolen property and mail fraud violations. After a two week trial, each subject was convicted on 12 counts. One subject was sentenced to 9 years in prison, and the other 5 years. United States District Court Judge Alfred J. Lechner, who presided over the trial, stated that there are few crimes with regard to monetary theft that could reach this magnitude. Judge Lechner added that the subjects attempted to compromise years and years of research undertaken by the victim companies.

In contrast, in December, 1993, the FBI, working with the Naval Criminal Investigative Service arrested two individuals who sold propriatary bid and pricing data to an FBI undercover agent. The two individuals had conspired to sell Hughes Aircraft bid and pricing data on an upcoming bid for the Tomahawk Cruise Missile Program to an individual they believed to be employed by McDonnell-Douglas for 50,000 dollars.

At the time both McDonnell-Douglas and Hughes manufactured the Tomahawk Cruise Missile for the United States Navy (USN). However, beginning in 1994, the USN was to award the contract to a sole vendor, either Hughes or McDonnell-Douglas. This updated Tomahawk Cruise Missile contract was valued at $3 billion, and was to have been awarded in June, 1994. This restructuring of the contract created an extremely competitive atmosphere between the two companies, and both conceded that loss of the contract would have closed down their missile facilities.

One individual was charged with Conspiracy to Deprive the U.S. of Its Right to Honest and Competitive Bidding on Contract (18 USC 371) and Aiding and Abetting (18 USC 2). The other was charged with Wire Fraud (18 USC 1343) and Aiding and

Abetting. In April, 1994, both defendants plead guilty to the charges against them. Notwithstanding the gravity of the offenses, in June, 1994, one was placed on probation for only one year and ordered to participate in the home detention program for 60 days. The other was committed to the custody of the U.S. Bureau of Prisons to be imprisoned for a term of only four months, with credit for time served, and only four months of home detention.

These and other problems underscore the importance of developing a systemic approach to the problem of economic espionage. I believe that only by adoption of a national scheme to protect U.S. proprietary economic information can we hope to maintain our industrial and economic edge, and thus safeguard our national security.

CONCLUSION

FBI investigations demonstrate that economic espionage perpetrated by foreign governments, institutions, instrumentalities and persons directed against the United States, establishments, corporations or persons in the United States is a critical national security issue which requires both a counterintelligence and law enforcement response. The FBI is in a unique position to address this issue, utilizing the authorities and jurisdictions assigned to both the FBI's Foreign Counterintelligence and Criminal Investigative Programs.

Since the initiation of the FBI's Economic Counterintelligence Program, the FBI has seen a 100 percent increase in the number of economic espionage-related investigative matters, involving 23 countries. This increase is primarily due to recent changes in the FBI's counterintelligence program and the concomitant emphasis on resources and

initiatives, but it also demonstrates that the problem is not a small one.

In order to maintain the health and competitiveness of critical segments of the United States economy, the development, production and utilization of proprietary economic information must be safe-guarded. The FBI will continue, as it has in the past, to utilize all available measures to protect this type of information from unlawful, illicit or clandestine collection by foreign powers. However, for the various reasons discussed, I believe a national scheme to protect proprietary economic information is warranted and necessary.

Director FREEH. I want to add also my compliments to the various Senators who have introduced bills. As you know, there is an Administration bill that is nearing completion. Hopefully that will be transmitted to the Congress very, very soon.

I thought what I would do in a few minutes is just try to outline for you the scope of the problem and what I see the gap to be with respect to a measured as well as an effective national response.

As you've cited, Mr. Chairman, the problem really involves billions of dollars and millions of jobs. It translates into industries being affected, people being displaced, and really the health of our national economy. I think today, more than ever, a strong national economy is really equivalent to national security. We've entered a phase and a century is about to be entered where our economic independence and security and strength is really identical to our national security, which is why this is such a critical issue for all of us.

The other point that I want to make is that we are not talking about, and certainly the bills that you've introduced do not contemplate, some new or novel Federal jurisdiction. Unlike many of the statutes that the FBI enforces, the authority for the protection of intellectual property and proprietary economic information really comes from the Constitution itself. It's not often that even the FBI can cite the Constitution as a basis for jurisdiction, but in article I, section 8, clause 8, the framers specifically set aside for the Congress the authority to make all necessary laws to protect intellectual property, or what today translates more specifically as trade secrets, critical technology ideas.

More than anything else the American economy has to sell to the world is its genius. The United States has become, in effect, the basic research lab for the world. It is estimated conservatively that $249 billion in basic research is spent in the United States by the Government as well as by industries. The issue before us today and the subject addressed in your legislation is really whether or not we should have a Federal law, a national policy, with respect to the protection of intellectual property and economic proprietary information from theft and misappropriation.

There is currently no such Federal scheme, and that's because of the way that the world has changed in 200 years, well beyond the contemplation of the framers. We live in cyberspace. We live in global economies. We live in a world of ideas, where those ideas can be instantaneously stolen, transmitted and taken to many places around the world where they can harm legitimate private as well as national security interests.

Let us just for a moment take a look at the various statutes that we have in effect which the FBI uses, and uses effectively in certain cases, to deal with this problem. We have, first of all, the Interstate Transportation of Stolen Property Act, which is in title 18. Ironically, that is the statute which is most usually applied or attempted to be applied when the theft or misappropriation of intellectual property or economic proprietary information is involved. Indicative of the problem, this was a statute that was passed in the 1930's in response to the fact that thieves were using automobiles to take stolen property—goods, merchandise and wares—from State to State, which was beyond the capability of many of the

local police departments to investigate. So, in effect, in 1995, on the threshold of the 21st century, we are really relying for most of our cases on the ITSP statute. As the Senator has pointed out, not only by case law—Dowling in the Supreme Court, Brown in the tenth circuit—but also by the interpretation and application of Assistant U.S. Attorneys, there's a real question whether downloading computer files, copying the information, and transmitting it somewhere is a theft—a theft, at least as contemplated in ITSP.

So we work very hard to investigate economic espionage activities using a statute which, when drafted, did not contemplate the kinds of problems and technologies that we're dealing with today. ITSP carries, by the way, a maximum penalty of 5 years' imprisonment.

Some of the other statutes that we use—the mail and wire fraud statutes, title 18, sections 1341 and 1343—again require, absolutely require, the use of wires or mails in the transmission of the property or instrumentality of the fraud. In many cases, we have investigated sets of circumstances where the nexus of mail and wire communications have not been used, and that is an absolute requisite for the application of those statutes.

Sections 1029 and 1030, which are the computer access and the computer fraud statutes, work in many instances very well. But, again, a lot of proprietary information is not transmitted either through computers, nor does it reside necessarily on computers. If someone steals the pricing information on a bid from a piece of paper sitting in some office, that would not have come within the confines of those two statutes.

The espionage statute, again, is not really applicable, because most of this information is not national security information.

So we are really left with a hodgepodge of statutes, which can from time to time be effectively applied. But what's lacking is one systematic Federal law which addresses the scope of the problem and doesn't depend on individual circumstances to assert jurisdiction. Let me just give you one quick scenario which we came up with. It's actually a set of facts relating to a case in 1990 involving the Mobil Oil Corporation. The scenario would run very briefly like this: A foreign nation is looking to build a nuclear reactor, a nuclear industry, and an American company wants to bid for $100 million worth of that contracting. Assume a profit of 20 or 25 million dollars, the hiring of many subcontractors, the creation of many jobs affecting communities as well as subindustries. What happens is an international information broker, as these thieves very ornately call themselves, finds a mole in that American company, an employee who is willing to steal the pricing information that goes to that corporation's bid. Now, that bid was worked up over hundreds and hundreds of work hours, at the cost of perhaps millions of dollars. It is confidential, it is sensitive. It is the classical example of proprietary economic information. Now, this employee, the mole within the company, gets access. Let's say he gets lawful access to that information, and not by way of a computer. He gives that information to this international information broker, who takes it to another country—not by wire or mail communication, but my personal trip—and delivers that to a foreign corporation, which by looking at the bottom line so to speak is able to un-

derbid and take that contract worth a hundred million dollars unfairly away from the American company, and does so using stolen or purloined or misappropriated economic proprietary information.

None of the statutes which I have alluded to would give us any jurisdiction with respect to that offense. And that is not, as I said, an atypical scenario for these crimes. Again, it's not a question here of some new novel or overwhelming jurisdiction that the Federal Government never had. It's simply keeping us apace with the technologies, the techniques, and the very active, targeted intelligence activity of many foreign companies and countries in this area.

The FBI has approximately 800 pending cases involving 23 foreign countries. These are State-sponsored economic espionage, forays and initiatives into the United States, using all the various techniques of intelligence officers and services, from compromising individuals, to unlawful wiretapping, to bribery, to all the things that these agents do and did, perhaps more so during the cold war where the objective was the ascertainment of military information.

Some of the cases that we have worked I can allude to with the absence of the foreign country involved, at least in this open hearing. This is just a sample list of companies that have been affected, by either State-sponsored economic espionage or espionage coming from other companies or corporations. We have IBM, Litton, Texas Instruments, Corning Glass, McDonnell Douglas, and the Schering-Plough and Merck case, which was a 1990 case. This is another good example of the issue of not only jurisdiction, but also penalties and deterrence. Schering-Plough and Merck, two drug companies, had spent approximately $750 million in research and development to develop some drugs. We had information that two individuals, one at each company, were willing to sell the R&D to the highest bidder. This would be the actual drug formulas. An undercover FBI agent, for $1.5 million, was able to get both drug fermentation processes—again R&D worth at least $750 million. The available statutes with which to prosecute again were relegated to the ones I previously referred to—mail fraud, interstate transportation of stolen property. If that had been a completed crime, the damage—just the monetary damage alone—would be absolutely staggering.

Other cases involve Motorola, the Ford Motor Company, and the Guidey case, which Senator Feinstein referred to, Hughes Aircraft—I could go on and on.

The incidence of these cases is also one that we find to be increasing, I think for a few reasons. One, in the wake of the cold war many of the foreign intelligence agencies have diverted some of their objectives from the military targets to the industrial, economic, and proprietary targets.

Second, after the cold war, many of our traditional military allies are now fierce economic competitors. So there is a great incentive to obtain U.S. proprietary secrets and information.

Third, there is a huge global market which can respond very quickly to early access and early production of items which require multimillion dollars of research and development. So there is a great premium on that R&D and on producing it very, very quickly.

The statutes that the two Senators, Mr. Chairman and Senator Kohl, have introduced, address many of the most immediate prob-

lems that we have. They address, for instance, the issue of confidentiality. As one of the members of the panel alluded to, many of these companies don't report these violations, because they don't want to go through a court procedure where they have to rely on whether or not a Federal judge may or may not grant confidentiality. So there is a great issue of having more damage and more economic harm by reporting a case like this than actually ignoring it and trying to absorb the damage.

The need for extraterritoriality is very important. In the Mobil case that I mentioned—a case that actually took place in London—the contact to the American company was through one of its employees in London. All of the activities took place in the United Kingdom. In a global world with global criminals, the extraterritoriality is, in my view, very, very necessary.

Most importantly, however, and as we have alluded to before, the concept of a systematic uniform Federal statute and program in this area is absolutely critical. Twenty-four States, including the District, have no trade secrets law with respect to any penalty or prosecution. Of the 25 States that have them, there is a hodgepodge of different penalties, theories, and jurisdictions. Very hard to come to grips with.

Finally, my last point would be I don't think we can rely on the private industry or the civil process to solve this problem. When I sat as a district judge in New York, where the docket is very heavy with trade redress cases and trade secrets cases, I often wondered at the financial ability of plaintiffs to come in and challenge these kinds of cases. The amount of discovery, the jurisdiction that is involved, as well as the uncertainty of the litigation, I think make this a problem which we can't simply relegate to the civil system where trade secrets have traditionally been enforced—at least for the last 200 years.

I also don't think we can rely on the States to take on a problem like this. This is really a national problem. If we're talking about foreign governments, we're talking about international activity and jurisdiction. I think it's a role for the Federal Government that Americans would not only understand but appreciate. As we said, it goes to jobs, millions of jobs, billions of dollars, and really the future health of our country.

So I certainly applaud the Senators for having this hearing. Mr. Chairman and Senator Kohl, the statutes that you've introduced, I think are a great start. I think there's tremendous support in industry. I've heard from many of the CEOs of Fortune 500 companies. I've spoken to my agents who are out in the trenches working these cases, and sometimes when they get a complaint, they don't know whether it's a counterintelligence case or criminal case, and it's hard to give them guidelines, because we don't really have a statute that addresses this problem head on.

So I think there's a great interest, a great need, and I certainly applaud your efforts.

Chairman SPECTER. Thank you very much, Director Freeh.

You characterize the problem very accurately when you talk about billions of dollars of losses and million of jobs involved. We're going to proceed now to 5-minute rounds, and I won't start my time until I finish the preliminary. I will yield first to Senator Kohl,

who's the author of the bill, with the acquiescence of Senator Kerrey, and then to Senator Kerrey and then our practice is to turn to Senators in order of arrival, so we will have Senator Feinstein, Senator Shelby, Senator Baucus, Senator Johnston, Senator Leahy——

Senator LEAHY. Mr. Chairman, I was the first person here. There was absolutely nobody here, and I waited, then I went over and met with Director Freeh——

Chairman SPECTER. Then the sequence of questioning will be Senator Leahy, Senator Specter——

[General laughter.]

Chairman SPECTER. Patrick, you've just moved up right behind Kerrey.

Senator LEAHY. Thank you.

Chairman SPECTER. And no affidavit is necessary.

Director Freeh, we heard from Director Deutch of the CIA last week on the international threat assessment and we took up the question of espionage. It is not the practice of U.S. intelligence agencies to engage in espionage activities and, in fact, when the CIA gets information about foreign corrupt practices by foreign companies, foreign governments, or espionage, their practice is not to turn over the information to the U.S. companies affected, but instead to turn it over to the Department of Commerce. That's a question we're going to have to take a close look at. You identified some 23 countries are engaged in economic espionage in some 800 cases. It is a matter of enormous importance.

I begin asking for your observations with the report that President Boris Yeltsin of Russia earlier this month—on February 7, just 3 weeks ago—instructed his espionage units to try to close the gap. Now, President Yeltsin is involved in a tough national election. It is not inconceivable that President Yeltsin might be looking to this as a means to bolster the Russian economy, although obviously in the short term that's not easy to do, but it might be something he would direct a lot of his attention to. If Mr. Yeltsin is to unleash the KGB or Soviet intelligence forces to work on industrial espionage, that could be quite a formidable array, given their international apparatus and their capability for military spying.

What is your assessment as to the potential damage which could occur if Yeltsin really goes at this hammer and tong—not to say hammer and sickle?

Director FREEH. I think it's an ominous sign whenever a foreign intelligence service prioritizes in any way the theft or stealing by espionage, particularly using sophisticated, clandestine means the economic secrets and proprietary interests of another nation. American corporations are not equipped to defend against that kind of an attack. That's the best argument in the world for a strong Federal law and policy with respect to dealing with the foreign State-supported espionage. I think using the techniques that certainly the SVR and the GRU are capable of using, but also all the other 22 countries currently engaged in economic espionage, presents a very formidable, very ominous threat to this country, to the infrastructure, to our economy. On top of these, the American companies, as good and sophisticated as they are, are not prepared, nor should they be, to deal with that kind of an attack.

Chairman SPECTER. When Boris Yeltsin makes a statement like that, really laying down the gauntlet, should there be something more than just defense that we play against that? Should there be some formal response by the U.S. Government to say that's not appropriate? Take it up in the diplomatic channels, as well as playing defense on investigations or prosecutions?

Director FREEH. Yes, I think that's appropriate to respond to. You can simply cite GATT and the TRIPS statutes and treaties, which I believe Russia is a part of, which protect and guarantee that from country to country, the rights of intellectual property holders are preserved. The title of ownership is honored and respected no matter where in the world it's distributed, and I think on a diplomatic level, those arguments could be made very forcefully.

Chairman SPECTER. Director Freeh, I'm not advocating that we use our CIA or our FBI as Boris Yeltsin is suggesting that he's prepared to use the intelligence ring and economic espionage. As I've already said in our intelligence committee hearings with Director Deutch, that alternative has been discounted. But should we give some consideration to fight fire by fire if we really find that foreign intelligence units are making deep inroads into our proprietary interests? Again, I emphasize I'm not suggesting it, but is it worth at least consideration?

Director FREEH. I think it certainly is. I think one measured response would be the type of statute that you and Senator Kohl have proposed. If we can start arresting these foreign agents, many of whom do not have diplomatic immunity, if we start arresting some of these foreign intelligence service officers not for overstaying a visa or for straying outside of their confines, but for engaging in a crime which between the two statutes would range from a 15- to a 30-year penalty, I think that's a very effective response.

Chairman SPECTER. Along the collateral lines of economic espionage, an idea which has been suggested by Senator Johnston as he and I were working on some proposed legislation involves the foreign corrupt practice issue. Our laws, applied appropriately, prevent our companies from bribing a foreign governmental official to get a contract there, but other countries do not have such laws, and other countries will tolerate their companies going into a foreign land, offering a bribe of a foreign official for a contract. I'd be interested in your evaluation of the scope of that problem.

Director FREEH. I think we are the only country that has such a law in the world. It does put us at a relative disadvantage. On the other hand, it does embody what is the first principle for our business ethics, our legal structures here, which is that all information and contracting opportunities ought to be done competitively but very fairly. I think it probably is a matter that needs to be taken up somewhat like the GATT and the TRIPS agreement on an international level. It's been tried before, it's not met with a lot of success, as you both know, but I don't think that is a reason for backing down.

Chairman SPECTER. Well, my red light is on, so I shall not pursue it now. But beyond GATT, Senator Johnston and I are pursuing some legislation which would give extraterritorial jurisdiction. This would make it a violation of U.S. criminal laws, if we can get

our hands on the companies which are competing with American companies and bribing foreign governmental officials to get their contracts.

I now turn to Senator Kohl.

Senator KOHL. Thank you very much, Senator Specter.

Director Freeh, of course, as you are aware, a company that has information stolen from it can often bring a private civil suit against the thief. So could you tell us why these civil suits are inadequate and why you think we need a criminal?

Director FREEH. I think in many cases, and having seen some of these cases myself as a judge, the cost of litigation, the expense of mounting litigation, the discovery, all of the involvement with respect to pre- and actual litigation is so enormous that many small companies, small entrepreneurs, and individuals could not be expected to mount such a civil action.

In another problem area, the jurisdictional bounds are not quite clear. There is State legislation in some places. There are serious questions about conflicts of laws. There's a serious issue about whether there would be any pre-emption or not with respect to some of the Federal statutes and theories that they would move under.

And I think perhaps the best argument is the fact that if you have an instance of foreign State-sponsored economic espionage, we're asking a small, mid-sized, or even a large corporation to go up against not only a foreign government, but a foreign intelligence service, which is not going to be amenable to discovery and all the other things which our legal process contemplates.

So I think it's really a national problem where we shouldn't rely on what we have for 200 years, which is our civil forum, to solve that problem. I don't think it protects people.

Senator KOHL. All right.

Director Freeh, in the case of individuals who work in an industry or at a company for many, many years and then switch jobs, they have in their mind all kinds of things that they know about—the company that they work for, the industry that they work for—and then they go to work for a competitor. How does that person know or how will that person know what it is he can take with him to his new job by way of all the information that he has accumulated, and how will he not know—or how will he know that he's not going to be prosecuted and put in jail for things that he might bring to his new job by way of information or ideas, and what kind of confusion and concern will that cause on the part of people who go from one job to another in the same industry?

Director FREEH. I don't think it should cause confusion, and I think it should be an area where prosecutors very carefully look at facts and use their discretion as they currently do. Your particular statute, for instance, very clearly defines what proprietary economic information is. It also specifically requires stealing, theft, misappropriation—in other words, the intent element of that statute is very, very strong.

If the subject recklessly or negligently reveals information that he or she learned in the course of employment, that would not meet the legal requirements of intent. If, however, there is a clear intent to steal and an intent to harm the owner, as your statute requires,

I think those are guidelines that prosecutors can follow quite easily.

Senator KOHL. All right.

Director Freeh, we understand that often companies are reluctant to sue people who steal information because they're afraid that all the secret information will be spilled out in the courtroom. Our bill contains provision to assure privacy. But as a former judge, can you tell us what you think about the secrecy provisions in our bill? Do you believe that companies really can be assured that their information will be protected when the U.S. Attorney brings a suit?

Director FREEH. I think with the provisions that are included in both bills—one is a requirement, the other one is a strong command—I think both of those bills would give the corporations certainly more confidence than they have now in going down a road where they really have to rely on the—I shouldn't say "whim"—but on the decision of judges without any guidance as to whether or not a set of circumstances requires confidentiality. I think the provisions in your bill with respect to confidentiality are essential, and I think the corporations would be much more amenable to coming forward and reporting crimes with that type of protection.

Senator KOHL. All right.

As you know, one bill focuses on foreign government theft, the other on individuals, and it includes, of course, American citizens. Is there any reason why we should be any less tough on American citizens than we would be on foreign governments?

Director FREEH. I think with respect to that issue, both bills would certainly be effectively used against Americans in the United States or in an extraterritorial capacity, who steal such information with the intent to harm the owner. I think both bills cover that area very, very well.

With respect to adding the element of aiding a foreign government or corporation, that's probably an issue, as we've discussed with your staff, that has to be ironed out in the framework of the GATT and the TRIPS agreement. As you know, under the GATT treaty, article 3 requires that the governments, all the signing governments, treat their nationals on the same basis they treat their foreign citizens or foreign corporations. There is a GATT question raised by that very issue and I'm confident that the committee counsel and the other people who you'll hear from will be able to work that out. But it is a very important issue to be resolved.

Senator KOHL. Our bill provides penalties of up to $10 million for a corporation that steals information. Do you think that that's high enough, or in some cases are corporations going to see that as a reasonable price to pay for the cost of doing business and for the information that they might be getting?

Director FREEH. That's a good question. If we're talking about a $750 million savings in RSD, it becomes almost de minimis to pay that kind of a price. I think, however, some forfeiture provisions and the discretion that sentencing judges would have under the guidelines might be able to bridge that gap. But I think you're absolutely right. We're talking about extremely high values here, and I think that certainly has to be addressed, either by a forfeiture provision or by some accommodation in the guidelines provisions.

Senator KOHL. Thank you very much, Director Freeh, Mr. Chairman.

Chairman SPECTER. Thank you, Senator Kohl.

Senator Kerrey.

Vice Chairman KERREY. Director Freeh, I'd like to focus a little bit on the threat and particularly like to come at it from the standpoint of current efforts, especially in the area of espionage, where we already have laws on the book and we're not really talking about changing it. Perhaps it might be useful to learn from you some of the problems that you're facing when you're confronting espionage.

As I understand it, the estimates of 51 or so countries that spy actively on the United States, and that the FBI has 23 investigations—23 countries under investigation at the moment. These are countries that are much more difficult to deal with, in some ways, than individuals. So we have 23 countries. These are not just foes like Russia. These are friends, traditional military and political friends, as well as neutral countries. As I understand it, there has been an increase in the number of those cases, espionage cases, from approximately 400 last year to 800 this year.

What I'd like to ask you, there's sort of a double-barrel question. First, does it have any impact on our ability to get those countries to stop when there's a leak and a disclosure that we were using electronic surveillance for the Japanese in negotiations with them.

And second does—does this increase from 400 to 800 reveal something that might be useful for this committee as we try to evaluate what our law should be?

Director FREEH. In two parts.

With respect to the leak, it is quite damaging and very compromising to have that kind of a leak. We're talking about the one last month with respect to the trade negotiations. It does certainly undercut and compromise the ability of both the intelligence agencies and the law enforcement agencies to do what they're empowered to do, which is to counteract active attempts by foreign intelligence services to obtain very sensitive trade negotiation information, which is used to undercut and compromise the United States' positions.

Vice Chairman KERREY. Just to follow up on that, I mean, we do not as a practice and policy of the President's directive, engage in economic espionage. But the question is, if it's disclosed, in this case illegally disclosed by someone that we were using electronic surveillance in the process of negotiation, is it not difficult then to go to an ally and say, "We're not using that information for economic espionage." In other words we're trying to persuade, are we not—the United States is trying to persuade not just foes, not just historical enemies, but historical friends and neutral countries that economic espionage needs to be prohibited worldwide. I'm just—I'm trying to elicit a slightly additional response on that particular question.

Director FREEH. I wasn't—I wasn't clear enough. What I was trying to say was—if the objective of that intelligence operation on our side is to counteract, from a counterintelligence point of view, the work of that foreign service or that foreign government to take our trade negotiation strategy, to take it by clandestine means, through

their intelligence services, through their corporations, if our objective is to counter that attack by using electronic surveillance or other means, I think that's quite appropriate. I don't think that is in the class of using our intelligence service to steal another country's proprietary information. It's a counterintelligence operation.

Vice Chairman KERREY. I understand that. I'm just saying that if I'm the Japanese government and you're the American government, it's going to be difficult for me to necessarily believe that you're merely collecting that information for negotiations and that you're not passing it on to a corporate interest that might benefit from it. We do not do that as a consequence of Presidential directive. But I'm just—we need not to discuss this further. I just wanted to make clear that I think it does undercut and make it difficult for us to get governments, which typically, as I understand, is what we're trying to do, we're trying to get governments to cease and desist in using economic espionage for government-owned companies, for government transactions, which is precisely what President Yeltsin was proclaiming as a part of their policy.

Can you talk to me a little bit, talk to us a little bit about the reasons for an increase——

Director FREEH. Yes.

Vice Chairman KERREY [continuing]. A doubling from 400 to 800 cases?

Director FREEH. I think one reason is the increased focus and resources that we've put on it. In 1994, I initiated a new program with respect to economic espionage counterintelligence, as well as the working of criminal type cases, whether derived from an intelligence source or otherwise, which would lead to the prosecution of subjects, whether they be Americans or foreigners engaged in blatant or very damaging types of economic espionage. So part of it is a new focus on our part.

The other—the other reason for the increase, I think, as several studies that I've cited in my statement reflect, is that industry, now more than ever—260 percent more in the Fortune 500 companies since 1985—are reporting these incidents to the FBI, and to the different components of the Justice Department. We have not in the past gotten that kind of a response.

So I think the answer to your question involves the combination of those two factors and the increased efforts and initiatives of the FBI with regard to investigating the State sponsored economic espionage.

Vice Chairman KERREY. Can you just briefly, because the light's going to flash off here in a minute——

Director FREEH. Yes.

Vice Chairman KERREY [continuing]. Can you briefly state whether or not governments are increasing their efforts in economic espionage in your view?

Director FREEH. Yes, in my view they certainly are.

Vice Chairman KERREY. Friendly governments, neutral governments, as well as traditional opponents?

Director FREEH. Yes. Both allies and adversaries.

Vice Chairman KERREY. In some cases they actually have laws on the books to encourage it?

Director FREEH. I don't know about that. I'd have to do some research with respect to that, and I will. But they certainly have increased their activities and operations in the United States against American companies.

Vice Chairman KERREY. Thank you.

Chairman SPECTER. Thank you very much, Senator Kerrey.

Senator Leahy.

Senator LEAHY. Thank you, Mr. Chairman.

I was concerned as I read through the report by the Computer Systems Policy Project at some of the things in it. The report quotes one U.S.-based manufacturer who said we lost a major procurement in a Middle Eastern country by a very small margin, this to a State-subsidized European competitor. They said they were clearly breached. "Our unique approach in financial structure appeared verbatim in the competitor's proposal." It cost 3,000 jobs, $350 million.

Another person said they had a multiyear, multibillion dollar contract stolen off their PC while they were bidding in a foreign country. They said had it been encrypted the foreign competitor could not have gotten it in time for the bidding frame.

Last year, as I mentioned earlier, Senator Kyl and Grassley and I introduced the National Information Infrastructure Protection Act to increase protection for what we keep on our computers. The current Computer Fraud and Abuse statute only protects from unauthorized access, classified information, financial institution computers, government computers and network computers that are infected with computer viruses.

We would expand the law to protect information in both private and government computers attached to interstate or international networks from theft or sabotage. Would the amendments that are in our bill, help you in fighting economic espionage that occurs over computer networks?

Director FREEH. They certainly would, Senator. Any expansion in the various intellectual property protections would advance that. Expansions in the copyright statute would be another example.

The issue, however, is, I think as I stated before, that is really one part, maybe an integral part, but really one part of the arena or one part of the universe that is really the subject of vast forms and different modifications of economic espionage, but that provision in particular——

Senator LEAHY. That's one part that can help.

Director FREEH. It's one part that would certainly help.

Senator LEAHY. I want to commend you for what you and the FBI have done in going after these areas of economic espionage. We read very little of it. They're not as glamorous as some spectacular crime where people see it happening, but you know and I know, and certainly from what you've briefed us in other fora, big amounts of money are involved, and the amounts of damage are enormous.

I'm wondering if the FBI has investigated companies where the trade secrets or the proprietary information that's been stolen had been encrypted. A corollary to that; should American firms use stronger encryption technology to protect what they have in their computers?

Director FREEH. I have not seen any cases where the theft involved information or trade secrets which were encrypted, to answer your question specifically. Of course, as the most recent study cited in my statement reflects, most of the corporate reported breaches with respect to economic security come from trusted onboard employees who, even under an encrypted system——

Senator LEAHY. Who may have the key to the encryption.

Director FREEH. Would have the key to the system. But I think it's certainly a good point to consider.

Senator LEAHY. Senator Cohen has a bill, S. 1525, which would make the new economic espionage crime a predicate offense under RICO prosecutions. The other two bills on the issue would not. Do you think the new economic espionage crimes should be a RICO predicate?

Director FREEH. My own view is that it should be a RICO predicate. All of the other statutes that we're currently using—the mail and wire fraud statute, even ITSP; in fact, both of the computer access statutes, 1029—are all RICO predicates. It seems that if we're coming in with a statute as comprehensive as this, we certainly would want to have it as a RICO predicate. That's my own view.

Senator LEAHY. I've worn a couple of hats here, one as a member of this committee and actually serving on this committee with Senator Specter, and then as a member of the Intelligence Committee for 8 years, serving with him there. I go back and forth on the question of being defensive in our nature. You speak of the economic counterintelligence as being purely defensive, not to collect economic information about foreign corporations to give to competing U.S. companies.

Then we find, of course, that we have, as has been brought out already, a former head of the French external intelligence services, a well-known Russian leader speak of the fact that intelligence services of those nations are being used to acquire American technological information.

Are we in a position where we should be re-examining this purely defensive American response?

Director FREEH. I think it's a subject of an ongoing debate, but I think, at least currently, the agreement and the consensus, at least with the people in the law enforcement and intelligence services that I speak to, is that we ought not to cross that line. I mean, there are a lot of things that foreign intelligence services do, including assassinations, that are abhorrent even to our clandestine activities. They certainly should be. To use our intelligence services to, in effect, be private investigators for corporate America, I would certainly recommend against that. I think it's a bad policy.

Senator LEAHY. If we made it a crime for foreign governments to engage in economic espionage against American companies, can we assume that a similar law quickly gets passed in their countries?

Director FREEH. Well, oddly enough, I'm told most of those countries have such laws.

Senator LEAHY. They do?

Director FREEH. In France, for example, I've been advised if you steal a trade secret from a company and give it to another French national, it's a 10-year penalty. If you give it to a foreigner, it's a 30-year penalty. Many countries—I think we're the only country,

certainly the only industrialized country that I know of, that does not have a national trade secret, intellectual property protection statute.

Senator LEAHY. We don't come up with any disadvantage by passing such laws.

Director FREEH. I don't think so at all.

Senator LEAHY. Mr. Chairman, I have other questions I'd like to submit for the record, because I'm supposed to be at another committee meeting. Also for the second panel.

Chairman SPECTER. Thank you very much, Senator Leahy. We'll submit your questions, and I'm sure the witnesses will submit written answers.

Senator LEAHY. Thank you.

Chairman SPECTER. Thank you, Senator Leahy.

Senator Feinstein.

Senator FEINSTEIN. Thank you, Mr. Chairman.

It is my view that economic espionage is a major problem. I am very pleased by your comments. I think it's very important that we indicate to our allies that we are not going to tolerate it in every way, shape or form. I think to, you know, not give this the kind of importance that it deserves is a mistake. So I'm very pleased to hear what you have to say, Director Freeh.

I have watched the envelope of the first amendment being pushed in this country for decades now to where you can tell somebody on the Internet how to make a bomb. They can actually—to have youngsters blown up. And, oh, there's a big debate about whether this should be possible or not. Now, in this field, you have people coming in and actually destroying companies by economic espionage.

I just read the proprietary definition in the bill, and it would appear to me that it's a very strong definition and a good definition. Have you read it, and do you concur?

Director FREEH. Yes, I've read it and I do concur. I think it also answers the question of defining the limits for people so innocent or negligent people don't run afoul of the criminal statutes.

Senator FEINSTEIN. Right.

Now, let's go on to another thing. As I understand it, your draft bill would include just espionage practiced by foreign nationals, in other words, and not domestic. Is there a reason why you do not apply your approach to domestic economic espionage?

Director FREEH. Again, you know, going back and forth between those two elements, Senator Kohl's bill and Senator Specter's bill, my view is that the greatest threat really emerges from the State-sponsored economic espionage. It doesn't mean that the other offenses should go untreated. It doesn't mean that they're not very serious. But from a national security point of view and from a law enforcement point of view, and given limited resources, which everyone in this room is painfully aware of, that's the best place where we could focus our attention. However, as I mentioned before, there may be a serious issue with respect to GATT, which would make that kind of discrimination contrary to our treaty obligations. So it's something that we need to deliberate on.

Senator FEINSTEIN. Because my position would be I think we ought to deal with them both. So I like the fact that the bill deals with both of them, both economic—both foreign and domestic.

Let me ask another question on the threshold amount of $100,000. Since this has to be proven beyond a reasonable doubt, it would seem to me that a threshold number is important. Your draft bill, I'm told, does not have a threshold number in it. Could you tell me what the reason for that is? Would you support a threshold number? And if so, what do you believe should be that amount?

Director FREEH. The only—I guess the only reservation I would have about a threshold would be that there would be a class of cases, and perhaps some important ones, where, because of the nature of the crime—perhaps it was only an attempt; perhaps it was a conspiracy that never went anywhere—the valuation of the property in question or the property acquired might fall below the $100,000, but a prosecutor and a jury might feel very strongly that that would be worthy of a conviction.

On the other hand, a threshold has the benefit of giving some guidelines to the prosecutors. In many of our criminal statutes, particularly in the bank fraud area, although the statute doesn't prescribe a certain amount of money, the U.S. Attorneys, say, for instance, in California, they will only take a bank fraud case over $100,000. So those thresholds are good. They focus resources and they exercise some discretion. But I think you can make a good argument either way for it.

Senator FEINSTEIN. Would there be any way of getting at the case that I think you mean; in other words, a very serious attempt but the proprietary information quite possibly would not have a value of over $100,000 at the time it was taken? You'd have to prove that in a court of law. Is there any other——

Director FREEH. I think you could prove it. You could value the asset or the economic information without actually having the subject take possession of it. I just think there would be some cases where a threshold like that could prevent a prosecutor from exercising discretion. My view—having been a prosecutor for 10 years, I probably bring a bias to this—is that we ought to give prosecutors broad discretion in deciding what cases to take and what cases not to take. I think they exercise that very well.

Senator FEINSTEIN. So you're saying in this area it would be preferable to take the threshold out.

Director FREEH. I think, in terms of flexibility and giving prosecutors more discretion, I would be in favor of that.

Senator FEINSTEIN. Thank you very much.

Thanks, Mr. Chairman.

Chairman SPECTER. Thank you very much, Senator Feinstein.

Senator Kyl.

Senator KYL. Thank you, Mr. Chairman.

Director Freeh, as always, we appreciate your crisp and knowledgeable testimony. Do you understand this legislation to include prohibitions on sabotage as well as theft? I don't know the answer to that. We seem to have a conflict here as to whether it's the case or not. And I don't mean to have you have to look it up.

Director FREEH. I'm actually just going to look at one definition. I don't think we contemplated sabotage, per se. On the other hand—all right, this is not my own knowledgeable or crisp answer, but I'm told by one more competent than I that under section 571, subprovision 3, it also prescribes the alteration or destruction of proprietary economic information or conveyances. So that certainly would cover the destruction of computer codes or other sabotage.

Senator KYL. Would the insertion of a bug, for example—fit that?

Director FREEH. It would be an alteration.

Senator KYL. OK, heads are nodding behind you.

In any event, we should make sure that the language is sufficiently broad to cover that, I would think.

Director FREEH. Good point.

Senator KYL. Would you concur?

Director FREEH. Yes, sir.

Senator KYL. OK, thank you.

Would there be a role for the State Department under this legislation in its no foreign policy objection requirement? Would that requirement still be extant in certain situations?

Director FREEH. I don't think—again, I'm not 100 percent sure about this, but I think if we had the criminal statute, at least the one contemplated by both Senators, it would not be a no-objection context, at least as the State Department has traditionally applied it, where there is no such statute.

Senator KYL. What would the FBI do differently if this legislation were enacted? How would you operate differently? Would you approach your investigations in cases differently?

Director FREEH. I think the first thing we would do is we would assign some more resources to these cases, because we have more of a certainty with respect to effective prosecutions. We would have a program that has a national impetus as well as a focus which we don't currently have. I think what we would also be able to do quite effectively is take a lot of the information that we collect in the counterintelligence area, also information that the intelligence agencies collect, and apply it, with all of the protections to sources and methods, but apply it in a criminal context. In other words, take some of that information that we have and use it, use it effectively, under a statute that gives us much broader prosecutorial discretion. So I think you'd see more prosecutions taking advantage of the intelligence information, which now may not fit within the pigeonholes of one of the available statutes.

Senator KYL. Do you need additional legislative authority to assist in the prosecution of the cases in order to protect the sources and methods?

Director FREEH. I think the CIPA protections would also govern with respect to these kinds of prosecutions. I also think the confidentiality provisions would go a long way to solving that problem. I don't think you would need additional specific legislation.

Senator KYL. Senator Leahy mentioned the legislation that he and Senator Grassley and I have introduced, which is yet another component dealing with computers. And as I understand it, there are some holes in the current law. For example, the transportation across State lines, definitions dealing with products or goods may not—in fact, under case law, apparently does not contemplate in-

formation. And I gather from your earlier statement that you would appreciate our acting on that legislation as well.

Director FREEH. Yes, Senator, it does fill a gap. It's very important testimony.

Senator KYL. Thank you. Again, thank you for your testimony. Thank you, Mr. Chairman.

Chairman SPECTER. Thank you very much, Senator Kyl.

I want to put into the record now a letter which I received, which the committee received just last night, from the Assistant Secretary of Defense in response to a letter which I had written on January 31 which followed up on a letter which had been written by Mr. Abe Foxman of the Anti-Defamation League. The letter that I wrote to Secretary of Defense Perry stated in part, "We have just noted the memorandum which purports to have a series of 'documented incidents,' relating to alleged Israeli espionage against the United States." That memorandum states, referring to the DOD memorandum, "The strong ethnic ties to Israel present in the United States, coupled with aggressive and extremely competent intelligence personnel, has resulted in a very productive collective effort."

Then my letter to Dr. Perry goes on to say, "Even if there are some individual incidents, that broad, blanket statement certainly constitutes the smear of guilt by association, suggesting dual loyalty."

In the earlier portion of that memorandum, the following is stated, and this refers to the DOD memorandum. Quote: "Many of our friends, military friends, are our economic-industrial threats. Some of these countries we deal with on a day-to-day basis." That refers to France, Italy, Israel, Japan, Germany, the UK, et cetera. The DOD memorandum then only refers to six incidents relating to Israel, and then my letter to Secretary Perry concludes:

> We request specific information on the statement as to the alleged, "low-ranking individual," that the DOD attributes these statements to. The six incidents cited on Israel strongly suggest that it is more than a casual memorandum initiated at a low level. We request specification on the background of the individuals involved, and whether those individuals' activities constitute a justifiable basis for the assertion on "strong ethnic ties."

As is not unusual, no response was received to that letter until the eve of this hearing, last night, as I am advised. The staff met with representatives of the Department of Defense to pursue this issue, and had—on February 20—propounded specific questions. I am going to make all of this a part of the record. We want to read a very short portion of their response.

> The department can attest that many foreign intelligence services attempt to exploit ethnic or religious ties. While the Israelis may have also attempted to exploit ethnic and religious ties with Jewish Americans, it does not follow that these Americans are necessarily any more susceptible to external exploitation than any other class of American citizens. The fact that ethnic targeting does not equate to ethnic susceptibility, to cultivation by foreign intelligence service, cannot be overstated. Any implication drawn from the CI profile that Americans would commit treason against the United States because of their Jewish heritage would be patently incorrect. The not so delicate implication to the contrary that some might draw after having read the Cl file is what the Department of Defense has stated previously as being particularly repugnant.

The letter to me from Emmett Paige, Jr., the Assistant Secretary of Defense references here his conclusion that he must, "defer our

final response until after completion of the ongoing internal review of this matter."

It's a little hard to understand how long it takes to have a response. While the issue of economic espionage is obviously one of enormous importance, allegations have to be handled with the greatest of care without any smear of guilt by association. The full context of these documents will be placed in the record. I would have commented on it earlier, but I just saw it as this hearing began.

Director Freeh, again we thank you for coming in.

Director FREEH. Thank you.

Chairman SPECTER. We commend you for your activities and the activities of the FBI. Each time we take a look, your responsibilities are increased. We appreciate your coming in. I'd like to talk to you briefly before you leave about another incident of particular concern to the Intelligence Committee.

Senator Cohen could not be with us today as he had to Chair a hearing with the Special Committee on Aging. However, Senator Cohen did submit an opening statement and he asked that it be submitted for the record, and without objection, his statement will be placed in the record at this point.

[Copies of the letters referred to and the prepared statement of Senator Cohen follow:]

January 25, 1996

Anti-Defamation League®

The Honorable William J. Perry
Secretary of Defense
The Pentagon
Washington, DC 20301-1155

Dear Mr. Secretary:

It has come to our attention that a Department of Defense memorandum has been circulated which warns American defense contractors to keep an eye out for Israeli spies and which attributes Israel's success in obtaining intelligence partly to the "strong ethnic ties to Israel present in the U.S."

Mr. Secretary, this is a distressing charge which impugns American Jews and borders on anti-Semitism. We believe an apology by the Department is needed. We think it is critical that the memorandum be removed from circulation and you indicate that in no way do the views expressed represent those of the Defense Department and the American government.

In addition, we are disturbed by the general tenor of the memorandum considering the fact that Israel is America's longtime ally, considering the fact that only five years ago Israel refrained from taking military steps against Iraq despite Scud missile attacks because its U.S. ally asked for restraint. One would hardly sense this alliance in the tone of the memorandum.

We wonder whether Israel is being singled out and, if so, why? Are similar memoranda written about other countries?

In sum, we find the memorandum a matter of serious concern. We respectfully urge your immediate attention.

Sincerely,

Abraham H. Foxman
National Director

AHF:saj

Anti-Defamation League of B'nai B'rith, 823 United Nations Plaza, New York, NY 10017 (212) 490-2525 FAX (212) 867-0779

ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

29 January 1986

Mr. Abraham H. Foxman
National Director
Anti-Defamation League of B'nai B'rith
823 United Nations Plaza
New York, New York 10017

Dear Mr. Foxman:

Dr. John P. White, Deputy Secretary of Defense, asked that I respond to your concerns regarding the preparation and distribution of a memorandum on Department of Defense letterhead referencing purported intelligence activities by the government of Israel.

I want to stress that the content of this document does not reflect the official position of the Department of Defense. The memorandum was inappropriately initiated by a low ranking individual at a field activity of the Defense Investigative Service. While we object to the document in general, singling out ethnicity as a matter of counterintelligence vulnerability is particularly repugnant to the Department.

We regret the publication of this material and took action in December to stop further distribution. We are notifying recipients that the document has been canceled. We have instructed appropriate personnel that similar documents will not be produced in the future.

In conclusion, I share your concern regarding this matter. You have my full commitment that we will do all that is necessary to preclude future incidents of this nature.

Sincerely,

Emmett Paige, Jr.

January 30, 1996

The Honorable William J. Perry
Secretary of Defense
The Pentagon
Washington, DC 20301-1155

Dear Mr. Secretary:

We appreciate Assistant Secretary Paige's prompt response to the letter I addressed to you last week, and welcome the Defense Department's assurances that "the memorandum on Department of Defense letterhead referencing purported intelligence activities by the government of Israel...does not reflect the official position of the Department of Defense." We especially appreciate the statement that "singling out ethnicity as a matter of counterintelligence vulnerability is particularly repugnant to the Department."

Nevertheless, we remain disturbed that such views could exist anywhere in the Department, and that such a memorandum, even though it has now been "cancelled," could ever have been circulated as Department policy. In our judgement, it is not sufficient for the Department to "instruct appropriate personnel that similar documents will not be produced in the future." To give weight and emphasis to the Department's disavowal of the content of this memorandum, we urge you to initiate an internal investigation in order to identify and reprimand those responsible.

By responding honestly and forthrightly to my first letter, you have indicated an understanding of the depth of our concern regarding this memorandum. We hope and anticipate that you will now take the crucial next step and institute specific measures to ensure that any Department staffer, at any level, whose conduct impugns the integrity of American Jews will face serious sanctions.

Sincerely,

Abraham H. Foxman
National Director

AHF:mes

cc: Emmett Paige, Jr., Assistant Secretary of Defense

Anti-Defamation League of B'nai B'rith, 823 United Nations Plaza, New York, NY 10017 (212) 490-2525 FAX (212) 867-0779

R-95%

ADL

MARK A. EDELMAN
Director, Marketing and Communications

MYRNA SHINBAUM
Director, Media Relations
Contact: Myrna Shinbaum (212) 490-2525, ext. 7747

FOR IMMEDIATE RELEASE

ADL ACCEPTS DOD ASSURANCES THAT MEMO IMPUGNING ISRAEL AND AMERICAN JEWS AS SPIES IS NOT POLICY; URGES INTERNAL INVESTIGATION

New York, NY, Jan. 29 . While the Anti-Defamation League (ADL) today accepted assurances by the Department of Defense (DOD) that it was moving to correct the damage done by a DOD memorandum stating that Israel may be engaged in espionage and that their current success in obtaining intelligence may be partly attributed to the "strong ethnic ties to Israel present in the United States," it called on the DOD to conduct an internal investigation into the matter.

Emmett Paige, Jr, Assistant Secretary of Defense, in responding to ADL National Director Abraham H. Foxman's letter to Defense Secretary William Perry said, "I want to stress that the content of this document does not reflect the official position of the Department of Defense," and that "while we object to the document in general, singling out ethnicity as a matter of counterintelligence vulnerability is particularly repugnant to the Department."

Mr. Foxman said that while he "accepts and appreciates the assurances from the DOD," he is "disturbed that such views would exist in the Department and that such a memorandum could be circulated as Department policy." He urged the DOD to "immediately initiate an internal investigation into the matter so as to reprimand those responsible and prevent a similar occurrence in the future."

As first reported in the February 1996 issue of *Moment Magazine*, the DOD memorandum was circulated to American defense contractors to be on the lookout for Israeli spies and referencing their "strong ethnic ties" in the United States. "I find the memorandum a matter of serious concern," Mr. Foxman wrote to Secretary Perry, and "this a distressing charge that impugns American Jews and borders on anti-Semitism."

The Anti-Defamation League, founded in 1913, is the world's leading organization fighting anti-Semitism through programs and services that counteract hatred, prejudice and bigotry.

###

USNFAX:YO-96

To: All Cleared Employees From: Deb Kornyak SECURITY IS KEY****HELP SPREAD OUR WINGS, NOT OUR TECHNOLOGY! Subject: Counterintelligence Briefing .fe off

****

DoD NEWSLETTER

COUNTERINTELLIGENCE INFORMATION

****

The Defense Investigative Service (DIS), as part of their education program, has started to send us Country Counterintelligence Profiles (see the one on Israel below). We feel it is important to provide you this information, but in no way are we implying that all your foreign contacts are trying to obtain classified and proprietary information from you. The purpose of this education is to heighten your awareness to prepare you for this type of encounter, whether it comes from a US citizen or foreign national.

Counterintelligence Awareness is critical to [our company's] success, and to our country's economic competitiveness. Many of our military "friends" are our economic/industrial threats. Some of these are countries we deal with on a day to day basis (ex: France, Italy, Israel, Japan, Germany, UK, etc.). Although we have always been aware of the necessity of protecting government classified material, we must understand our company proprietary information is just as valuable in the wrong hands.

The FBI, CIA, NIA, DODSI, DOE, NSA and DIS Counterintelligence, etc., are banding together to gather and disseminate counterintelligence information to the National Counterintelligence Center (NACIC). Never before has this type of threat data been assembled by the Government and shared with industry on a real-time basis.

Successful espionage operations are seldom discovered until it is too late, which many times results in devastation to the company. In the past, many companies were reluctant to provide information on espionage for fear of the potential effect on the company name, products, stock, marketability, etc., so it has been difficult for the government to capture $'s lost. With the recent increase in awareness through industry and government openness, it is obvious that there is far more economic and industrial espionage than previously suspected.

Please notify me immediately if you feel you have been approached by someone soliciting personal/work related information from you beyond what would be expected in a normal contact, and I will process the information through the proper channels. What may seem insignificant to you, could be the missing piece of a bigger puzzle.

****

OPEN SOURCE COUNTRY COUNTERINTELLIGENCE PROFILE

COUNTRY: Israel

KEY JUDGMENTS:

o Israeli espionage intentions and capabilities are determined by their traditional desire for self reliance.

o Israel aggressively collects military and industrial technology. The US is a high priority collection target.

o Israel possesses the resources and technical capability to successfully achieve its collection objectives.

BACKGROUND: Non-traditional Adversary

Israel is a political and military ally of the US, however, the nature of espionage relations between the two governments is competitive. The Israeli's are motivated by strong survival instincts which dictate every facet of their political and economic policies. This results in a highly independent approach determining those policies which they consider to be in their best interests. Consequently, the Israeli's have established an intelligence service capable of targeting military and economic targets with equal facility. The strong ethnic ties to Israel present in the US, coupled with aggressive and extremely competent intelligence personnel, has resulted in a very productive collection effort. Published reports have identified the collection of scientific intelligence in the US and other developed countries as the third highest priority of Israeli Intelligence after information on its Arab neighbors and information on secret US policies or decisions relating to Israel.

The primary Israeli collection agencies are the Mossad, (equivalent to the CIA), Aman the Israeli military Intelligence Branch, and a little known agency identified as the Lakam which translates to the Science and Liaison Bureau. It has been reported that the Lakam was disbanded after it was identified as the agency responsible for recruiting and running Jonathan Pollard. However, there is no doubt that the Israeli intelligence community has adjusted its collection efforts and continues to closely target the scientific and industrial community with the US.

John Davitt, formerly the head of the Justice Department's Internal Security Section was quoted as stating the Israeli intelligence services were "more active than anyone except the KGB...They were targeted on the US about half the time and on Arab countries about half the time."

METHOD OF OPERATION/TECHNIQUES:

The Israeli Intelligence service employs traditional collection tools. It has a trained agent cadre well versed in espionage tradecraft. Collection requirements are identified by the national leadership based on factors relating to defense and the national economy. The most compelling requirement deals with immediate threats to the existence of Israel posed by its geographic neighbors. Therefore, collecting information relating to the existence of nuclear, chemical, and biological weapons are the first order of priority. Israeli personnel are always seeking to recruit knowledgeable human sources with access to this information. Recruitment techniques include ethnic targeting, financial aggrandizement, and identification and exploitation of individual frailties. Selective employment opportunities (placing Israeli nationals in key industries) is a technique utilized with great success.

DOCUMENTED INCIDENTS:

o The most highly publicized incident involving Israeli espionage directed against the US is the 1985 arrest of Navy Intelligence analyst Jonathan Pollard. Pollard conveyed vast quantities of classified information to Israel for ideological reasons and personal financial gain.

UPDATE (11/22): JERUSALEM - The government agreed on Tuesday to grant citizenship to Jonathan Pollard, who is serving a life sentence in the US for spying for Israel. Pollard hopes Israeli citizenship will improve his chances for early release. The government ruling came on the 10th anniversary of Pollard's arrest outside the Israeli Embassy. Israel has sought clemency in the past, but Pollard hopes the granting of citizenship could bolster that request because the government will now be acting on behalf of a citizen.

o In 1986, Israeli agents stole proprietary information from Chicago based Recon Optical Inc., an Illinois optics firm. Significant financial damages were incurred by Recon, and in 1993, the Israeli's agreed to pay three million dollars in damages.

o In the mid eighties, a large DoD contractor hosting Israeli visitors experienced the loss of test equipment during field testing relating to the manufacture of a radar system. Two years later, a request was received from Israel to repair the piece of missing equipment.

o In 1994, a small firm utilizing a proprietary PC based product to upgrade Israeli radar systems sent an engineer to Israel with its product. Upon arrival, the PC based equipment was malfunctioning. Examination by the engineer traveling to Israel revealed the proprietary chip had been tampered with.

o Israel is suspected of furnishing the Peoples Republic of China with US export controlled technology desired by the Chinese to upgrade their indigenous capability to develop a fighter aircraft.

o Author Peter Schweizer maintains Israeli Air Force personnel have repeatedly gained access to TOP SECRET military research projects by paying off Pentagon employees.

INFORMATION DESIRED:

The Israeli's have a voracious appetite for information on intentions and capabilities relating to proliferation topics i.e., nuclear, chemical, and biological weapons. Specific types of technology desired includes avionics equipment, spy satellite data, theater missile defense information. Israel has developed an arms industry which produces weapon platforms for each branch of its military service. Information relating to the technologies relative to these platforms is actively sought. Israeli industry manufactures the Merkava Mark III battle tank, the Sa'ar class corvette missile boat, and the Kfir jet fighter. US firms engaged in research, development, and manufacturing associated with these technologies together with radar and missile defense technologies are high priority collection targets.

Debra L. Hornyak Manager, DoD Security Administration/PSO
MD/0374 X2541 (OMGVMJ HORNYAK) /

WASHINGTON D.C. OFFICE

Anti-Defamation League®

TRANSMISSION MEMORANDUM

Telecopy to the following number: 224-1772

The following document is for:

Name: Jim Wolfe

Firm: ____________________

From: Jess Hordes

Total number of pages to be transmitted, including this one: 9

Date: __________ Time: __________ (a.m.)/(p.m.)

ATTENTION:

This communication is intended only for the use of the addressee and may contain information that is privileged and confidential. If you are not the intended recipient, you are hereby notified that any dissemination of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately by telephone and return the original facsimile to us at the above address via the U.S. Postal Service.

Anti-Defamation League of B'nai B'rith, 1100 Connecticut Avenue, N.W., Suite 1020, Washington, D.C. 20036
(202) 452-8320 • FAX: (202) 296-2371

Counterintelligence Profile

[redacted]

COUNTRY:

ISRAEL

KEY JUDGMENTS:

- Israeli espionage intentions and capabilities are determined by their traditional desire for self reliance.

- Israel aggressively collects military and industrial technology. The United States is a high priority collection target.

- Israel possess the resources and technical capability to successfully achieve its collection objectives.

BACKGROUND:

Non-traditional Adversary

Israel is a political and military ally of the United States. However, the nature of espionage relations between the two governments is competitive. The Israeli's are motivated by strong survival instincts which dictate every facet of their political and economic policies. This results in a highly independent approach determining those policies which they consider to be in their best interests. Consequently, the Israeli's have established an intelligence service capable of targeting military and economic targets with equal facility. The strong ethnic ties to Israel present in the United States coupled with aggressive and extremely competent intelligence personnel has resulted in a very productive collection effort. Published reports have identified the collection of scientific intelligence in the United States and other developed countries as the third highest priority of Israeli intelligence after information on its Arab neighbors and information on secret U.S. policies or decisions relating to Israel.

The primary Israeli collection agencies are the Mossad, equivalent to the CIA, Aman the Israeli Military Intelligence branch and a little know agency identified as the Lekem which translates to the Science and Liaison Bureau. It has been reported that the Lekem was disbanded after it was identified as the agency responsible for recruiting and running Jonathan Pollard. However, there is no doubt that the Israeli intelligence community has adjusted its collection efforts and continues to closely target the scientific and industrial community within the United States.

John Cavitt formerly the head of the Justice Department's Internal Security Section was quoted as stating the Israeli intelligence services were "more active than anyone but the KGB.... They were targeted on the United States about half the time and on Arab countries about half the time."

METHOD OF OPERATION/TECHNIQUES:

The Israeli intelligence service employs traditional collection tools. It has a trained agent cadre well versed in espionage tradecraft. Collection requirements are identified by the national leadership based on factors relating to defense and the national economy. The most compelling requirement deals with immediate threats to the existence of Israel posed by its geographic neighbors. Therefore, collecting information relating to the existence of nuclear, chemical, and biological weapons are the first order of priority. Israeli personnel are always seeking to recruit knowledgeable human sources with access to this information. Recruitment techniques include ethnic targeting, financial aggrandizement, and identification and exploitation of individual frailties. Selective employment opportunities (placing Israeli nationals in key industries) is a technique utilized with great success.

DOCUMENTED INCIDENTS:

a. The most highly publicized incident involving Israeli espionage directed against the United States is the 1986 arrest of Navy intelligence analyst Jonathan Pollard. Pollard conveyed vast quantities of classified information to Israel for ideological reasons and personal financial gain.

b. In 1988 Israeli agents stole proprietary information from Chicago based Recon Optical Inc., an Illinois optics firm. Significant financial damages were incurred by Recon and in 1993 the Israeli's agreed to pay three million dollars in damages.

c. In the mid eighties a large DoD contractor hosting Israeli visitors experienced the loss of test equipment during field testing relating to the manufacture of a radar system. Two years later a request was received from Israel to repair the piece of missing equipment.

d. In 1994 a small firm utilizing a proprietary PC based product to upgrade Israeli radar systems sent an engineer to Israel with its product. Upon arrival the PC based equipment was malfunctioning. Examination by the engineer traveling to Israel revealed the proprietary chip had been tampered with.

e. Israel is suspected of furnishing the Peoples Republic of China with U.S. export controlled technology desired by the Chinese to upgrade their indigenous capability to develop a fighter aircraft.

f. Author Peter Schweizer maintains Israeli Air Force personnel have repeatedly gained access to top secret military research projects by paying off Pentagon employees.

INFORMATION DESIRED:

The Israeli's have a voracious appetite for information on intentions and capabilities relating to proliferation topics i.e. nuclear, chemical, and biological weapons. Specific types of technology desired includes avionics equipment, spy satellite data, theater missile defense information. Israel has developed an arms industry which produces weapons platforms for each branch of its military service, information relating to the technologies relating to these platforms is actively sought. Israeli industry manufactures the Merkava Mark III battle tank, the Sa'ar class corvette missile boat and the Kfir jet fighter. United States firms engaged in research, development, and manufacturing associated with these technologies together with radar and missile defense technologies are high priority collection targets.

SOURCE OF INFORMATION:

1. Friendly Spies, by Peter Schweizer
2. The Washington Times
3. The Dallas Morning Herald
4. The Washington Post
5. International Defense Review
6. Every Spy a Prince by Dan Raviv and Yossi Melman
7. Foreign Intelligence Organizations by Jeffery T. Richelson

[redacted] is an Industrial Security Representative with the Defense Investigative Service in Syracuse, New York. The document on Israel which was taken entirely from the listed open source material reflect his interpretation of the articles and do not necessarily represent the views of the Defense Investigative Service or the Department of Defense.

United States Senate

SELECT COMMITTEE ON INTELLIGENCE
WASHINGTON, DC 20510-6475

January 31, 1996

SSCI #96-0436

The Honorable William Perry
Secretary, Department of Defense
Washington, DC

Dear Secretary Perry:

We have just noted the memorandum which purports to have a series of "documented incidents" relating to alleged Israeli espionage against the United States. That memorandum states:

> "The strong ethnic ties to Israel present in the US, coupled with aggressive and extremely competent intelligence personnel, has resulted in a very productive collective effort."

Even if there are some individual incidents, that broad, blanket statement certainly constitutes the smear of guilt by association suggesting dual loyalty. In an earlier portion of that memorandum, the following is stated:

> "Many of our military 'friends' are our economic/industrial threats. Some of these are countries we deal with on a day to day basis (France, Italy, Israel, Japan, Germany, UK, etc.)"

On the copy of the memorandum provided to us by the Department of Defense, there are no purported "documented incidents" for any of those countries except Israel. Please advise us whether there are such "documented incidents" as to the other countries which were identified: (France, Italy, Japan, Germany, UK)

We have noted a paragraph in the letter from Assistant Secretary Emmett Paige, Jr., to Mr. Abe Foxman dated January 29, 1996:

> "I want to stress that the content of this document does not reflect the official position of the Department of Defense. The memorandum was inappropriately initiated by a low ranking individual at a field activity of the Defense Investigative Service. While we object to the document in general, singling out ethnicity as a matter of counterintelligence vulnerability is particularly repugnant to the Department"

We request specification on the statement as to alleged "low ranking individual." The six incidents cited on Israel strongly suggest that it is more than a casual memorandum initiated at a low level. We request specification on the background of the individuals involved and whether those individuals' activities constitute a justifiable basis for the assertion on "strong ethnic ties."

We request your prompt response.

Sincerely,

Arlen Specter
Chairman

J. Robert Kerrey
Vice Chairman

BY TELEFAX

ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

February 27, 1996

COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE

Honorable Arlen Specter
Chairman
Select Committee on Intelligence
United States Senate
Washington, DC 20510-6475

Dear Mr. Chairman:

Your letter of January 31, 1996, to the Secretary of Defense has been referred to me for reply. Your letter requested information concerning a memorandum prepared on Department of Defense (DoD) letterhead relating to Israeli intelligence activity and my reply of January 29, 1996, to the National Director of the Anti-Defamation League (ADL) of B'nai B'rith.

The quotation contained in your letter that identified six friendly foreign countries was part of an introduction or preamble produced by a Defense contractor - it was not prepared or distributed by the Department.

The purported "documented incidents" contained within the memorandum provided to you by the Department were included within a Profile that pertained only to the State of Israel. We have previously gone on record publicly as having stated that the Profile does not reflect the official position of the Department of Defense.

With regard to your request for specificity concerning my letter of January 29 to ADL National Director Foxman, I must defer our final response until completion of the on-going internal review of this matter.

As you know, Ms. Dempsey, my Deputy for Intelligence and Security, met with staff representatives of your committee the morning of February 20 to assist in your inquiry into this serious matter. The information requested during that meeting is enclosed.

I trust the foregoing information, including that appended hereto, provides a satisfactory interim response to your inquiry. Please be assured that the Department of Defense considers appropriate handling and resolution of this matter to be of the utmost importance. A separate response has been provided to Senator Kerrey.

Sincerely,

Emmett Paige, Jr.

Enclosure

Department of Defense Response to Questions Posed during Meeting with SSCI Staff on February 20, 1996

Does the implementing guidance required by E.O. 12968 disqualify employees for access to classified information if they are vulnerable to ethnic targeting?

No. By way of background, the "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information" was approved in July 1995 by the Security Policy Forum. It serves as the basis for making decisions for access to classified information throughout the Federal government.

Although the adjudicative guidelines do not address ethnic targeting, per se, there are two related criteria - foreign influence and foreign preference. Potentially disqualifying and mitigating factors under those criteria are included within the Guidelines.

The foreign influence criterion addresses issues that must be considered when a candidate for a security clearance, regardless of ethnic origin, has immediate family members, or others to whom the clearance applicant is bound by obligation or affection, who are non-U.S. citizens or may be subject to duress by a foreign interest, regardless of the country involved. Such a situation could create the potential for influence or duress that could result in the compromise of classified information. Contacts with citizens of other countries or financial interests in other countries are also relevant to security clearance determinations if an applicant could reasonably become vulnerable to coercion or other forms of exploitation.

The foreign preference criterion addresses the situation where an individual might act in such a way as to indicate a preference for a foreign country over the United States. Examples of possible disqualifying activities in this regard range from the active exercise of dual citizenship to voting in foreign elections to foreign military service.

What is the meaning of the term "very productive collection effort" as it relates to "strong ethnic ties to Israel present in the United States" contained within the Counterintelligence Profile on Israel?

By way of context, this question refers to the sentence, "The strong ethnic ties to Israel present in the United States coupled with aggressive and extremely competent intelligence personnel has resulted in a very productive collection effort," found in the first paragraph of the "CI Profile."

It would be inappropriate to discuss here the relative success or productivity of foreign intelligence collection efforts aligned against the United States. The Department can attest that many foreign intelligence services attempt to exploit ethnic or religious ties. While the Israelis may have also attempted to exploit ethnic and religious ties with Jewish Americans, it does not follow that these Americans are necessarily any more susceptible to external exploitation than any other class of American citizens.

The fact that "ethnic targeting" does not equate to "ethnic susceptibility" to cultivation by a foreign intelligence service cannot be overstated. Any implication drawn from the CI Profile that American Jews would commit treason against the United States because of their Jewish heritage would be patently incorrect. The not so delicate implication to the contrary that some might draw after having read the CI Profile is what the Department of Defense has stated previously as being particularly repugnant.

Institutionally, what has the Defense Investigative Service (DIS) done and what does DIS intend to do to provide more meaningful classified threat information to industry?

For many years the Intelligence Community was criticized for withholding useful foreign intelligence threat information from legitimate consumers. Some knowledgeable individuals attributed this alleged reluctance to a cultural aversion and fundamental distrust of appropriate, non-intelligence community consumers, particularly private industry. Eliciting from the Intelligence Community, specifically counterintelligence (CI) organizations, threat information necessary to support coherent, risk-based security countermeasures, military operations, and industrial activity was arguably ad hoc and sporadic.

The Joint Security Commission recognized this shortcoming and recommended that the DCI's Counterintelligence Center serve as the executive agent for "one-stop shopping" for CI and security countermeasures threat analysis. The goal was to seek a national-level focal point for threat analysis that would be easily accessible by government and industry to support broad security management decisions. Pursuant to Presidential Decision Directive/NSC-24, the National Counterintelligence Center (NACIC) was established in 1994 to guide all national-level CI activities, including countering foreign economic and industrial intelligence collection activities.

The CI office established within DIS in 1993 was created to sensitize cleared companies under Defense security cognizance to the foreign intelligence threat and to provide more effective and efficient support to the CI community in discharging its long-standing personnel security and industrial security responsibilities. For example, DIS participates with the FBI on DECA briefings throughout the country and, as a customer service, attempts to augment security briefings with tailored threat information that industry has sought for so many years.

The initial challenge for DIS was to become regarded by both the intelligence and counterintelligence communities as a legitimate consumer of threat information, especially as it relates to the defense contractor establishment. Following that, DIS became increasingly involved in serving as a purveyor of threat information to defense contractors. Nonetheless, there has been a persistent belief on the part of many defense contractors that the threat information being made available to them did not meet their needs to compete effectively in the global marketplace.

This purported dearth of meaningful threat information may have precipitated the wholly inappropriate preparation and distribution of the counterintelligence country profiles at issue. The proposition that meaningful threat information, classified if appropriate, may not be finding its way to appropriate industrial consumers is a matter under current review. Private industry remains the foreign collection target in most cases of economic espionage.

PREPARED STATEMENT OF SENATOR WILLIAM S. COHEN

Mr. Chairman, I would like to commend you for calling this hearing and for holding it in an open forum. Economic espionage, despite its great and growing significance, is a matter that has received far too little attention, and much of the attention it has received has fostered misimpressions.

All too often, that attention has focused on the hypothetical question of whether the United States should begin to conduct offensive action against foreign private companies, which I would oppose, and has failed to appreciate the degree to which foreign intelligence services conduct or support economic espionage against American companies—a threat that is not hypothetical but very real and increasingly damaging.

One of the reasons for the misunderstanding of this problem is that it has too often been treated as the domain of the defense and intelligence communities. This past week, the GAO issued a report on the threat to U.S. technology when foreign companies acquire U.S. defense contractors. While that threat is real, it is in many respects a comparatively minor issue because U.S. defense contractors are very aware of the espionage threat and have well-established mechanisms for defending against it. Save for large multinationals, however, non-defense companies in America are largely oblivious to the threat and undertake few if any precautions to protect themselves.

Over the last few years I have tried to move the discussion of these matters out of the closed-door settings of the Intelligence and Armed Services Committees and into the public domain. It was 2 years ago next week, in fact, that the Senate adopted an amendment I offered to S. 4, the National Competitiveness Act, requiring the President to submit an annual report on foreign industrial espionage modeled on the State Department's annual report on terrorism, which has done a great deal to increase media, and thus public, awareness of the terrorism threat. This was deliberately offered to the Competitiveness bill so that it would attract the attention of the business media, rather than the defense-oriented press, and so that the Commerce Committee would have jurisdiction over it and become a forum for congressional oversight of this problem.

While this reporting requirement unfortunately had to be moved to the intelligence authorization bill after S. 4 stalled in conference, I am pleased that the first annual report has resulted in more and better media coverage of the problem, which should lead to enhanced industry awareness and precautions. At the same time, the report relegated too much information to the classified appendix, not because release of the information would have put at risk sources and methods, but because it would have caused diplomatic awkwardness. Perhaps after today's hearing, it will be clear that if friends and allies are willing to play hardball by stealing from American companies, we should not be afraid to engage in the comparative softball sport of public telling the truth about their actions.

This report, however, is but one means of assisting U.S. industry in defending itself. In recent years, the State Department has worked to assist a select group of large companies and the FBI has worked to expand the Bureau's DECA (Development of Espionage, Counterintelligence and Counterterrorism Awareness) program to include nondefense companies. But I think it is an open question whether these efforts have been as effective as they need to be, particularly in assisting small and medium sized companies that often are the fount of much of our most advanced technology. A related question is how to involve other agencies such as the Commerce Department that are in the business of assisting U.S. industry and which have extensive contacts within the business community. These agencies' programs of assistance to industry provide ready-made vehicles for informing industry of the threat and means to protect against it.

Like the chairman and Senator Kohl, I have also been interested in improving law enforcement tools to pursue, prosecute and punish those engaged in economic espionage. During the Bush Administration, I spent months trying to get executive branch officials focused on what actions could be taken in this area and it was only in the closing days of the administration that the Justice Department agreed that legislation was needed to enable the Attorney General to counter economic espionage, particularly that conducted by foreign governments or by companies that are owned or assisted by foreign governments.

To their credit, Director Freeh and other Administration officials have taken greater initiative in addressing the problem, and the bills that Senators Specter, Kohl and I each have introduced reflect a great deal of dialog with and among interested officials in the administration. The bills Senator Specter and I have introduced regarding economic espionage conducted by or for the benefit of foreign governments are very similar in objective and construction. Perhaps Director Freeh will be able

to comment on their differences, such as the issue of vicarious liability, the inclusion of which I believe is favored by some Federal law enforcement officials to give them greater prosecutorial flexibility and reach and to enhance the deterrent effect of the legislation.

Senator Kohl's bill addresses the issue more broadly, including private sector-on-private sector espionage. As a result, his bill will be more controversial and require more deliberation. I view it as the second step in a sequential approach, with the first step being legislation along the lines that Senator Specter and I have offered and which I believe can be acted upon fairly expeditiously while debate continues on the broader legislation offered by Senator Kohl.

In closing, Mr. Chairman, let me again thank you for calling this hearing. As one who has worked this issue for many years and who will be leaving the Senate at the end of the current session, I commend you and Senator Kohl for taking an interest in this increasingly important problem and urge you to keep on pressing it in future Congresses. In doing so, I hope you will try to bring in our colleagues from Commerce, Banking and other relevant committees because the solution to this problem lies more in prevention than in prosecution.

Chairman SPECTER. We will now turn to our second panel today, which consists of two victims of economic espionage, Dr. Raymond Damadian, president of Fonar Corporation, and Mr. Geoffrey Shaw, former president of Ellery System, Inc., a Boulder, CO, software company. We also have here today Mr. Michael Waguespack, the Director of the National Counterintelligence Center, who will be available to respond to questions.

Gentlemen, we very much appreciate your coming. We will take just about a 2-minute break. I want to have a short conversation with Director Freeh, and then we will begin your testimony.

[A brief recess was taken.]

Chairman SPECTER. Gentlemen, we very much appreciate your coming in. We understand the difficulties of private companies coming forward with testimony of this sort, so we are very appreciative.

Mr. Damadian is the inventor of the magnetic resonance imager, MRI, a unique cancer detection device, my material says. It does more than detect cancer, I can testify to that personally, and I thank you for the MRI. I have been the beneficiary of it. For his success with the MRI, Dr. Damadian was awarded the National Medal of Technology in 1988, the highest honor in technology. The theft of his technology has been very troublesome.

We turn to you at this point, Mr. Damadian. We would like to put you on a 5-minute timer, as we have the committee members. So your full statement will be made a part of the record, and to the extent you can summarize within or close to that time limit, we would appreciate it, leaving the maximum amount of time for questions and answers.

The floor is your's.

[The prepared statement of Dr. Damadian follows:]

salary for the two years or until non-competitive employment is achieved. All entrances to the building are guarded and all briefcases are searched when employees enter and leave the building. No employee may leave the building with technical documents that do not possess a form signed by the president authorizing their transport. Video cameras are trained on all high tech areas within the company. The computers on which technical work is performed all have their disk drives, printers and modems removed so that technical information cannot be transmitted or copied.

Despite these precautions, the following are but a few examples of what has occurred.

1) A gypsy service company hired Fonar service engineers to provide them Fonar proprietary technology so that the gypsy company could service Fonar MRI machines. The service of Fonar MRI machines required the use of specially designed Fonar diagnostic software and trade secret schematics to troubleshoot the complex computer boards of the MRI. Fonar learned that the service vendor was in possession of Fonar proprietary schematics and software. In a civil proceedmg, Fonar sought injunctive relief in Federal Court. A temporary restraining order (TRO) was issued ordering the accused to cease and desist from any use of Fonar's proprietary software and schematics.

When the service contracts did not return to Fonar, we became concerned that the judicial order was being ignored. One Fonar user reported that their gypsy service company was continuing to service their Fonar scanner and was doing so with tapes marked Fonar Diagnostic Software. The user offered to reconnect the scanner modem so that Fonar could monitor the gypsy company's loading of its copyrighted diagnostic software on the scanner while the scanner was being serviced. With its modem connected. Fonar was able to monitor the service company from New York as it loaded Fonar's diagnostic software on the Fonar MRI scanner in New Mexico. In so doing, Fonar was able to capture the print screens that proved the illegal use of Fonar's software in direct violation of the judicial order restraining such use. Fonar sought a contempt of court ruling from the judge, which was granted.

While no meaningful sanctions accompanied the judge's contempt citation for the violator's indifference to a federal judge's order and no criminal sanctions were applied to deter others from continuing to steal the many millions of dollars of proprietary technology that this loss represented, Fonar objected. (Fonar ultimately learned at trial that the gypsy service company possessed an entire set of Fonar's drawings covering every aspect of the machine, as well as multiple copies of every module of Fonar's copyrighted diagnostic and operating software. All were presumed by the company to have been obtained from one or more of the former Fonar service engineers hired by the gypsy company.) The judge responded, "What do you expect me to do, put these people in

Testimony of Raymond Damadian, M.D.
President and Chairman, Fonar Corporation
110 Marcus Drive, Melville, NY 11747
Before the Senate Intelligence Committee
and Senate Judiciary Committee
February 28, 1996

Dear Chairman,

By way of introduction, I am the President of Fonar Corporation and an inventor We are a Long Island company that employs 300 and manufactures MRI machines, which we ship and install worldwide

Fonar introduced the first MRI scanning machine to the medical industry in 1978. I am the patent holder of the first patent for the MR scanning machine, which patent was filed with the U.S. Patent Office in 1972. I authored the first publication in Science magazine in 1971, that reported the discovery of the signal that enabled the MRI machine. In it I also proposed a full body scanner. Other independent scientists, principally Paul Lauterbur and Peter Mansfield, followed with further important contributions to the technology. My students and I built the first scanner and performed the first scan of a live human being in 1977. Using my original patent for its economic foundation, we formed Fonar Corporation in 1978 and in 1980 introduced the first commercial scanner that commenced the MRI industry

The path has not always been easy, Mr. Chairman. My patent was not enforced and that, coupled with severe losses of most of the rest of our proprietary technology through industrial espionage, describes an industrial environment in today's America that is not supportive of manufacturing enterprises that are badly needed to prosper our nation, namely patent protection and freedom from espionage.

Perhaps a few examples from our company's own experience make the point best.

All of our company's trade secrets are very carefully guarded. All schematics and engineering drawings are tightly controlled. Important documents are stamped Top Secret in large red letters and possess threatening messages of criminal prosecution if violated. A log is kept of all drawings and technical documents issued to employees. Each employee is required to personally sign for each drawing or document and to specify in writing when it is to be returned. He is required to sign his name in large letters across the entire face of every document he is issued. Each employee signs a confidentiality agreement at the time of employment in which he promises not to disclose any information for which he does not have *written* authorization to do so from the president of the company. Each technical employee signs an agreement as a condition of employment that he will not work for a competitor for two years upon leaving the company. The company reciprocates that in the event he cannot gain employment outside the field of MRI, the company will pay his

jail?" From Fonar's point of view the irony was that if the theft had been someone's $15,000 car, incarceration would have been automatic.

2) In another occurrence, a Fonar service engineer was hired by Toshiba, a direct manufacturing competitor. When the employee was reminded that he had signed an employment agreement in which he agreed not to work for a Fonar competitor for two years so that the competitor could not use him to acquire trade secrets and technology precious to Fonar, he expressed indifference to his commitment. Fonar had committed in this agreement that if he could not find employment outside of the MRI field, Fonar would pay his salary until he could do so for up to a period of two years. He took the Toshiba employment without further consultation with Fonar. When Fonar pursued its remedy in civil court, Fonar found that Toshiba had indemnified the employee from legal action and had agreed to pay all legal costs to defend against any legal action Fonar might bring.

3) In another occurrence, Fonar in protecting its technology, required a new user in Mexico to keep its premises locked at all times during the installation of the scanner so that competitors could not see the insides of the scanner's magnet and learn vital Fonar trade secrets. The user at Fonar's MRI installation dutifully complied. The magnet that Fonar was seeking to protect was a new iron frame design using permanent magnets that was a first in the industry. Many years after this installation, I met a Siemens executive who said he had been at the Mexican installation installing Siemens X-ray equipment when the Fonar scanner was being installed. Siemens is a large German multi-national company and a direct competitor of Fonar. Overcome with curiosity as to how Fonar magnets were creating their magnetic field, he requested to see the scanner during its installation and was denied by the Mexican manager in charge. The Siemens executive told me that a few nights later he overcame his difficulty and learned how our magnet was constructed. He explained to me that he invited the Mexican technician in charge of the installation out to dinner and filled him with alcobolic heverages. The technician than agreed to let him in to see the installation. He gained entry to the high security Fonar scanner site the same night and accomplished a full inspection of the interior of the Fonar MRI magnet.

4) In another instance, Fonar had a signed sales contract for $1,000,000 from a customer in Brooklyn and a $25,000 down-payment for a Fonar MRI scanner. Hitachi persuaded the customer to breach its sales contract with Fonar arguing that Fonar was a small company that could not maintain itself over the long haul. They then proceeded to sell the customer a magnet that was a copy of Fonar's basic permanent magnet design in direct violation of Fonar's basic magnet patents and broadly infringing them. When their magnet was installed, they encountered an unexpected problem -- the solution of which they had failed to acquire from Fonar. Their magnet was installed next to a large train track. The passing trains generated magnetic fields that interfered with the scanner's performance. Fonar had developed sophisticated feedback technology to cope with this common urban problem and the customer, had he proceeded with his Fonar installation.

would not have had to suffer from it. He did, however, have to suffer with it for the better part of a year and made his frustration known in the medical community. During this period, Fonar was receiving phone calls from a variety of outside sources seeking to find out how Fonar had solved the problem of the passing trains. Eventually the phone calls ceased. Not long after, we learned that Hitachi had overcome the problem. One of our engineers visited the Hitachi site in Brooklyn to see what Hitachi had done to solve the problem. He found an exact copy of our apparatus.

Altogether the above situation does not portray a happy situation for the American manufacturer who must fend off gigantic foreign competitors engaged in a feeding frenzy on America's internal markets without either patent enforcement or anti-espionage laws to protect him. The combined effects of these adverse circumstances can be seen on the chart I have attached. In 1992 the U.S. suffered a medical equipment trade deficit with Japan of $320,000,000. If my MRI patents had been enforced it would have been a year of trade surplus instead of deficit. The kind of destructive espionage I have described tilted the trade imbalance in medical equipment further against us.

The MRI is an American invention with an American patent. Today MRI is a multibillion dollar industry. Because Fonar's patent was not enforced, of the eight companies making MRI machines today, there are only two left that are American -- Fonar and GE. All the rest are foreign. They are Hitachi, Toshiba, Shimadzu, Siemens, Philips and Picker.

Our experience as a company has been that civil remedies are wholly inadequate in dealing with industrial espionage, particularly because of the severe mismatch between the personal economic resources of the larcenous employee and the enormity of the financial injury that the company sustains from his actions. Because of this mismatch, the company has no hope of being made whole from the employee's financial resources by civil action, especially if the employee has been indemnified by the company orchestrating the illegal acquisition.

The proposed legislation for effective criminal sanctions against individual or entities that seek to profit from industrial espionage appears to be the only means by which these noxious practices and the enormous economic destruction they bring upon the American economy each year can be curbed.

Diagnostic Imaging & Therapy Systems

Trade Balance

CALENDAR YEAR 1992 (in U.S. dollars)					
COUNTRY	EXPORTS	% Share	IMPORTS	% Share	BALANCE
Germany	301,638,699	14.95%	578,026,441	32.55%	(276,387,742)
Japan	264,670,735	13.12	585,495,403	32.97	(320,824,668)
Canada	167,714,703	8.31	22,832,903	1.29	144,881,800
Netherlands	143,067,845	7.09	168,253,096	9.47	(25,185,251)
France	139,053,469	6.89	123,562,901	6.96	15,490,568
United Kingdom	112,547,658	5.58	75,174,628	4.23	37,373,030
Italy	90,432,792	4.48	25,967,958	1.46	84,484,834
Australia	68,713,260	3.41	3,955,211	0.22	64,758,049
China	65,697,608	3.26	230,093	0.01	65,467,515
Brazil	59,351,337	2.94	6,928	0.00	59,344,409
Mexico	58,427,919	2.90	3,873,607	0.22	54,554,312
South Korea	52,492,524	2.60	3,653,817	0.21	48,838,707
Hong Kong	38,993,025	1.93	12,000,784	0.68	26,992,241
Belgium	35,464,619	1.76	22,388,550	1.26	13,076,069
Switzerland	34,039,311	1.69	15,763,755	0.89	18,275,556
Taiwan	29,607,240	1.47	2,268,816	0.13	27,338,424
Spain	29,148,523	1.45	9,970,803	0.56	19,177,720
Sweden	26,178,428	1.50	23,025,472	1.30	5,152,968
Argentina	24,046,114	1.19	10,100	0.00	24,036,014
Austria	20,289,187	1.01	7,862,878	0.44	12,426,309

Data Source: U.S. Department of Commerce, Bureau of the Census

TESTIMONY OF RAYMOND DAMADIAN, M.D.

Dr. DAMADIAN. Mr. Chairman, by way of introduction, I am the president of Fonar Corporation, a Long Island company that employs 300, and manufactures MRI machines. I hold the first patent for the MR scanning machine, which was filed in 1972, and my students and I built the first scanner and performed the first scan in 1977.

The path has not always been easy, Mr. Chairman. My patent was not enforced. That, coupled with severe losses of the rest of our proprietary technology by industrial espionage has made it impossible for us to build a prospering manufacturing company. Our experience has taught us that America's current industrial environment is not supportive of new companies trying to bring new inventions to market. Patent enforcement and freedom from espionage—the fundamental ingredients of such ventures—are all but non-existent.

A few examples from our company's experience make the point best. A gypsy service company servicing medical equipment hired Fonar service engineers, thereby acquiring a full set of top secret engineering drawings, and multiple copies of our copyrighted software. We obtained a temporary restraining order from a Federal judge ordering this group not to use Fonar schematics or software in the service of Fonar scanners. They ignored the judges order. Through a modem connection, we secured hard proof of them loading our diagnostic software on our scanner in violation of the judges order. The judge cited them for contempt of court.

When we complained there were no sanctions beyond the citation, the judge said, "What do you expect me to do, put them in jail?"

The irony is, if it had been someone's automobile instead of millions of dollars of technology, incarceration would have been automatic.

In another instance, Toshiba, a Japanese manufacturer of MRI machines and a direct competitor of Fonar's, hired one of our service engineers. We reminded the employee that he had signed a noncompete at the time of employment in return for his training. He ignored his commitment and joined Toshiba. When we brought an action to enforce our contract, we learned that Toshiba had indemnified him and was paying all his legal bills.

In another case, we learned how we lost valuable technology to a German company, Siemens. To protect the technology of our magnets, which was precious to our company, we required that all of our magnet installations take place behind locked doors. A Siemens executive proudly told me that that precaution was easily overcome. He reported that he took the technician out to dinner, filled him with alcoholic beverages, and thereby secured an invitation to enter the room and inspect the scanner for as long as he wished, which he did.

In another case, Hitachi reversed a sales contract on a scanner which we had already received a down payment on. The Brooklyn scanner site was next to a large train track, and Hitachi lacked the technology to cope with trains. Our company began receiving phone calls asking how Fonar coped with trains. We learned the customer was angry that passing trains were destroying his images. After

about a year, the phone calls stopped, and we learned the customers train problem was solved. One of our engineers visited the site. He found an exact copy of our train compensating apparatus installed on the Hitachi scanner.

All together, the conditions described do not portray a happy circumstance for the American manufacturer, who must fend off gigantic foreign corporations engaged in a feeding frenzy on American's multitrillion dollar domestic internal markets.

The combined effect of these adverse circumstances can be seen in the chart I have brought with me. I think you can see it. In 1992—there is a highlighted region directly to the right, which cites the trade balance with various foreign companies, and I particularly highlighted the trade imbalance with Japan. In 1992, the United States suffered a medical equipment trade deficit with Japan of $320 million. If my MRI patents had been enforced, this would have been a trade surplus instead of a deficit. Destructive espionage tilts the scales even more sharply against America.

The MRI is an American invention with an American patent. Today, MRI is a multibillion dollar industry. Because Fonar's patent was not enforced, of the eight companies taking sales out of the American market today, there are only two left that are American—Fonar and GE. All the rest are foreign. They are: Hitachi, Toshiba, Shimadzu, Siemens, Philips, and Picker.

Our experience as a company has been that civil remedies are wholly inadequate in dealing with industrial espionage.

The proposed legislation for effective criminal sanctions appears to be the only means by which these noxious practices and the enormous economic destruction they bring upon America each year, can be stopped.

Finally, Mr. Chairman, I wanted fervently, in the development of the MRI, to use my invention to build a great new multibillion dollar manufacturing enterprise for America, the same way that Edison and Bell did. I have found that even though I have now labored diligently for more than a quarter of a century, the tools for doing what Edison, Bell, Eastman, and others did, no longer exist. Indeed, we have had the disheartening experience that no amount of toil at creating new innovations could reverse the process. But that by a combination of willful patent infringements and industrial espionage, our innovations were stripped from us as fast as we could possibly create them.

Moreover, I believe you will not find my experience unique. Indeed, I sadly report I believe you will find it universal. I have sadly concluded, Mr. Chairman, that unless America quickly restores to its innovators the basic tools they need to build businesses, namely, effective patent enforcement, and protection from espionage, America will soon cease to exist as a manufacturing nation.

The economic cratering and threat to our national security that the loss of our manufacturing base to foreign nations will create, will be dire enough. The social upheaval that can be expected to follow in the wake of such a manufacturing demise, can be expected to jeopardize the very republic on which we stand.

I have come to Washington, not to regale Congress with this sad message on the unfortunate outcome of MRI, but to persuade Congress and the American people of the urgency of the matter, and

of the urgent need to restore the tools of patent enforcement and protection from espionage our nations manufacturers must have to compete.

Thank you.

Chairman SPECTER. Thank you very much, Mr. Damadian; thank you, indeed.

We now turn to Mr. Geoffrey Shaw. His former company, Ellery Systems, Inc., specialized in developing distributed computing technology, and following the theft of its unique software code, Ellery Systems, as I understand it, was not successful at pursuing existing Federal remedies.

Mr. Shaw, we welcome you here, and the floor is your's. Your full statement will be made a part of the record, and to the extent you can limit your opening testimony, we would appreciate it.

[The prepared statement of Mr. Shaw follows:]

Statement of Geoffrey Shaw
Former CEO of Ellery Systems, Inc.

Ladies and Gentlemen of the Senate Intelligence Committee and the Senate Judiciary Subcommittee on Terrorism and Technology, my name is Geoffrey S. L. Shaw. I am a Senior Partner of Global Commerce Link, LLC a successful Internet business software applications development and operations services company in Boulder, Colorado.

In 1994 I was the CEO of another Boulder software development company, Ellery Systems, Inc., that specialized in an area of commuting and communications technology development called Distributed Computing technology. At that time Ellery Systems was supplying software technology to government projects primarily involved in NASA astrophysics activities. Much of the early development of Ellery's technology was funded by DOD R&D contracts where the focus was on intelligence analysis applications, C3I, and related applications.

In 1994 our focus was on applying the experience gained deploying our technology in support of various NASA information systems applications to producing a library of applications that other developers in the commercial sector could use to build robust and innovative productivity applications for business and other markets. Based on the experience we had gained and the support we were receiving from other industry leaders to include Hewlett Packard, IBM, Digital Equipment, Sun Microsystems, and others, we had high hopes of commercial success.

Those hopes and years of hard work by some 25 employees were dashed two years ago, February, 1994, by what a subsequent investigation by the FBI indicated may have been an carefully planned, but poorly executed industrial espionage operation in which both hard copies and electronic copies of the source code for Ellery's software was stolen by an employee of Ellery Systems in collusion with other individuals including foreign government officials and the highest level of company management in a state company of a foreign government.

Was it in fact an espionage operation? We will never know. Was it, as the individuals subsequently repeatedly indicted by Federal Grand Juries, claimed merely an unfortunate "mistake"? We, the American people, and American industry will never know because the case never went to trial.

The facts of the case seemed clear. The defendants admitted taking Ellery's source code. They admitted meeting with government and company officials of a foreign country, in this case The People's Republic of China specifically to set up a deal in which they would receive $550,000 US dollars ostensibly to set up a company to use the technology they had taken from Ellery to produce applications and other products. They admitted entering into an agreement to provide this technology to a Chinese company in return for the above mentioned moneys. They admitted deleting copyright notices and other identifiers that would indicate that the software codes they had taken from Ellery were clearly Ellery's property. They admitted lying to Ellery officials when asked if they were in possession of any property of Ellery's.

And yet while these facts were verified and other evidence was uncovered by the FBI which would seem to indicate that this was not merely a case of theft motivated by greed, no federal statute existed with which to charge the perpetrators beyond a barely applicable wire fraud statute.

Had we known then what an enormous disadvantage we were actually at, we may have thought twice about bringing the case to the federal authorities attention. In fact it was not an easy decision to make anyway. We realized that doing so could have at least as many negative results for our small company as positive. Many company's that have been victimized by acts of industrial espionage do not come forward, and with good reason. The effect of coming forward can be devastating in terms of shareholder and consumer confidence, particularly if there is really nothing substantive that can be done about the matter.

Larger companies have the advantage of being better able financially to pursue civil remedies which can be a deterrent, to employ private investigators and security specialists to track down and negotiate settlement terms with individual perpetrators or to bring other influential, including politically influential support to bear in pursuit of claims that are made and pursued discreetly. Small entrepreneurial firms, i.e. the types of firms responsible for the vast majority of the innovation, new technologies and new jobs created in this country do not generally have those options.

So why did we come forward? Because though we knew there was real risk to our company by doing so, we believed and still believe that that risk is outweighed by our obligation to our customers, our industry, the community that we are a part of, and the larger society that is our nation. That is not self aggrandizing rhetoric ladies and gentlemen. A company paid with its life for assuming that position. 25 jobs no longer exist because of it. Man centuries of incredibly complex and hard work and millions of dollars of our own investment were at stake and we knew it. The company as a whole, that is the men and women who stood to loose the most by doing so, unanimously agreed that reporting and pursuing the case was the right thing to do. Those men and women put their dreams, hopes, visions and expectations on the line to defend what was theirs, just as they had put those things on the line the whole time they were engaged in inventing the technologies and applications that were stolen from them.

You see, when we discovered that our code had been stolen and how it had been stolen we immediately suspected that this might be a case of industrial espionage. We suspected that because we knew that our employee had just returned from a trip to China, though he told us before going that the purpose of that trip was to visit his mother whom he claimed was ill. Within days of returning he tendered his resignation. The next day our code was suddenly transferred to another company known to have ties to China.

Given that state of affairs we believed, and still believe that we had an obligation to inform the federal authorities.

Even so, when after just a few days we learned from the US Attorney that a wire fraud statute violation might be the only thing that could be brought to bear against the individuals who had stolen our property and that proving a case under that statute would be very difficult and possibly impossible, we almost decided to drop the whole thing and simply focus on recovering as best we could.

But when we learned of a letter that one of the defendants had sent to the chairman of the Chinese company ostensibly funding the operation in which the defendant stated that "the common practices of the Americans" should be used "to defeat them in their own competition;" we became determined to see the case through to whatever end it came to. You see Ladies and Gentlemen, at that point we realized that it was not just Ellery's future that was at stake. In fact it became clear to us that Ellery's fate was no longer really important when compared to what was at stake. That statement represents a direct attack on the American way of life that enables and encourages individuals and small groups of individuals to band together, invest whatever they have including their sweat, dreams and hopes, to create entire new industries and the entire new horizons that we, in this country, have come to expect will be created by young, entrepreneurial, put-it-all-on-the-line companies like Ellery Systems.

I ask you to remember Ladies and Gentlemen that this country was founded and grown by men and women who believed they had the right and the ability to do just that. American entrepreneurialism is not just a "business thing". It is not just a tradition. It is a way of life. Our economy depends on it. Our great companies are products of it. Thomas Edison, Henry Ford, Boeing, Westinghouse, Chevron, and most other companies here were started and built by entrepreneurs who had a dream, an idea and guts. In recent to very recent years companies that are household names today around the world including Apple, Microsoft, Hewlett-Packard, Sprint, MCI, Oracle, Sun Microsystems, Silicon

Graphics, Intel, Netscape Communications, America Online, Fidelity, RCA, Motorola, CNN, and the Colorado Rockies to name a very small sample, carry on that American way of life and create entirely new industries and opportunities for future generations to do the same. We absolutely assume that this way of life will continue to be available to individuals who chose to pursue it and that what those individuals dream will provide jobs and competitive opportunity for our children and theirs. As a nation and as a society we are betting our future on this way of life continuing.

Over just the past couple of years we have all witnessed this American phenomenon create yet more billions of dollars of new wealth and opportunity as we transform the Internet, which American innovation created, into a multi billion dollar industry that has already changed the way business, consumers and governments world wide view the world they live in.

It is this way of life; this tradition of encouraging individual and small company innovation from which almost all of what makes us so able to compete and lead in the fields we chose to pursue comes; this freedom and willingness to try and try and try again until we succeed that those cynical and chilling words threatened.

And so Ellery's employees decided to stand up and say that enough is enough. This kind of calculated and cynical attack cannot and will not be tolerated by those of us who put everything we have into creating the American Dream that those chilling words so directly threaten.

As I have stated, in the end no case was brought against any of the individuals who participated in taking Ellery's property and thus ended the life of a company that might have contributed even more than it did contribute to American innovation and industry. Because no case was brought, the individuals are not guilty of any crime and no crime can be attributed to them. They are innocent by definition and by right in the eyes of our

system and I completely and whole heartedly support that system in spite of how this case turned out.

Nothing I say should be interpreted as a condemnation of these individuals or of any other party to the events that led to my being here. The events which led to my being here are past and have been settled as well as our laws and system could settle them and I accept that and believe that our system actually worked by not prosecuting these individuals when there was, at the time no law under which they could be duly prosecuted.

However, I also believe that today, given the inevitability of this kind of thing continuing to happen as foreign espionage agencies and assets are used to conduct operations against American companies, that it is proper and appropriate for new federal legislation to be adopted that has real teeth and real deterrent effect against this kind of activity. Therefore I support and endorse the Specter-Kohl legislation and urge you to support it.

American technology companies, especially the small highly innovative companies that actually create most of the technology and jobs in the is country, are among this countries most valuable economic assets and they are a cultural and social asset we can all be proud of. They are quite simply this country's future. They don't need much and they don't want much. But they also don't want the intelligence agencies of the world thinking they can get away with declaring open season on them. Therefore I urge your support for this important legislation.

Ellery's fate is history. But we count our blessings. We found that the FBI and the US Attorney's office is both extraordinarily capable and admirably professional in the manner and rigor with which that can pursue these kinds of cases. We found that the support and encouragement we received from the community, from industry and from our elected representatives was unwavering and dependable. We found that our system worked even when we didn't like the result. And we found that we could go on and succeed by virtue of our own continuing hard work and our belief in ourselves and each other.

Today many of Ellery's former employees are Global Commerce Link employees. Those employees and their vision, creativity, innovation and shear courage reflect well on all of us. The American Dream is alive and very well at Global Commerce Link and at thousands of other incredibly creative, innovative, and courageous companies across the United States. Keeping it alive and well is something we all have a stake in.

Thank you.

TESTIMONY OF GEOFFREY SHAW

Mr. SHAW. Thank you, Mr. Chairman, madam.

My name is Geoffrey Shaw, and I am a senior partner of Global Commerce Link, a successful Internet business software and development operations company in Boulder, CO.

In 1994, I was the CEO of Ellery Systems, Inc., that specialized in an area of computing communications technology called distributed computing. Hopes of our commercial success and years of hard work by some 25 employees were dashed 2 years ago, almost to the day, in February 1994, by what a subsequent investigation by the FBI indicated was a carefully planned but poorly executed industrial espionage operation, in which both hard copies and electronic copies of Ellery's source code was stolen by an employee of Ellery Systems, in collusion with other individuals, including foreign government officials and high level company officials of a State-owned company of a foreign government.

The facts of the case seemed very clear. The defendants admitted taking Ellery's source code. They admitted meeting with the government and company officials of a foreign company, or a foreign country—in this case, the People's Republic of China. They admitted that the meeting was held specifically to set up a deal with which the defendants would receive 550,000 U.S. dollars, ostensibly to set up a company of their own to use the technology that they had taken from Ellery to produce applications and other products. They further admitted entering into an agreement to provide this technology and the products and applications that they and others developed with it, to the Chinese company that was ostensibly funding the operation.

We suspected that this might be a case of economic espionage, because we knew that our employee had just returned from a trip from China. We had been thoroughly briefed by the FBI over the years about these types of incidents. Within days of returning, our employee tendered his resignation. The very next day, our code was transferred to another company in the United States, known to have ties to China.

Given this state of affairs, we believed and we still believe that we had an obligation to inform the Federal authorities. Had we known then what an enormous disadvantage we were actually at, we may have thought twice about bringing the case to the authorities attention.

While the facts I have presented here were verified and other evidence was uncovered by the FBI that would seem to indicate that this was not merely a case of theft motivated by greed, we were informed by the U.S. Attorney that no Federal statute existed with which to charge the perpetrators beyond the barely applicable Wire Fraud Statute.

We almost gave up the whole thing. We considered that seriously. But when we heard that among the evidence recovered by the FBI was a letter to the chairman of the company in China in which one of the defendants stated that the common practices of the Americans should be used to defeat them in their own competition. At that point we were determined to see the case through regardless of what the effect might be on Ellery Systems.

You see, ladies and gentlemen, at that point we realized that it was not just Ellery's future that was at stake. In fact, it became clear to us that Ellery's fate was no longer really important compared to what was at stake. That statement represents a direct attack on an American way of life, a way of life that enables and encourages individuals and small groups of individuals to band together, invest whatever they have, including their own sweat, their dreams, their talents, their capabilities and their hopes, to create new industries, new technologies, and the very new horizons that we in this country have come to expect to be created from our technology and other innovative companies.

I ask you to remember, ladies and gentlemen, that this country was founded and grown by men and women who believed that they had the right and the ability to do just that, and that many of our great companies, to include Apple, Microsoft, Hewlett-Packard, Sprint, MCI, Oracle, Sun Microsystems, the Colorado Rockies, to name just a very few, are products of that tradition and that way of life.

Ellery's fate is history. But we count our blessings. We found that the FBI and the U.S. Attorney's office are both extraordinarily capable and professional in the manner and the rigor with which they can pursue these types of cases. We found that the support and encouragement we received from the community, from industry and from our elected representatives was unwavering and dependable. We found that our system worked, even if we didn't particularly like the result. And finally, we found that we could go on and succeed by virtue of our own continuing hard work and our beliefs in ourselves and in each other.

Today, many of Ellery's employees are employees of Global Commerce Link. Those employees and their vision, creativity, innovation and sheer courage reflect very well on all of us. The American dream that was under attack by those chilling words is alive and well in Boulder, CO, and in thousands of other communities populated with creative, innovative, and courageous companies across the United States.

Keeping it alive and well is something that we all have a stake in.

Thank you.

Chairman SPECTER. Thank you very much, Mr. Shaw. It is very distressing to hear your testimony.

We are going to be keeping the record open for an additional 48 hours, because we have been asked to do so by Kodak, IBM, Lockheed-Martin, and Hughes Corporation, all having indicated their desire to submit statements in support of this kind of legislation. I am hopeful that the public airing of this subject today will bring forward many more people with the kind of courage you display, willing to come forward to testify.

One initial question which comes to my mind is whether the provisions of GATT on the protections of patents would be of any significant help to you. Mr. Damadian, what do you think?

Dr. DAMADIAN. No. As a matter of fact, I think to the contrary; I think they were harmful to us because they changed the lifetime of the innovators patent from 17 years from the date of issue to 20 years from the date of filing, leaving the entire burden of the ex-

haustion of that time span on the burden of the patentee and whatever delays he encounters in the Patent Office. They can sometimes be as long as 15, 20 years before a patent issues. Gordon Gould's patents, for example, that were fundamental patents on the laser, one took him 18 years to get through the Patent Office—well, I don't think I need to go on with it, but I felt that the patent provisions in GATT were decidedly harmful to the United States.

Chairman SPECTER. Your point is well taken with respect to when you start to date the time running. But how about the aspect of obligating other countries to respect the patents. Do you think there is a significant likelihood that that will happen?

Dr. DAMADIAN. No.

Chairman SPECTER. You like a criminal sanction better?

Dr. DAMADIAN. Well, you know——

Chairman SPECTER. I think you should.

Dr. DAMADIAN. I think that—our experience has taught us that—there's another element in this that I didn't say in my testimony, but one of the problems that you deal with when the only remedy is a civil remedy, is that there is a fundamental economic mismatch between the perpetrator of the crime and the magnitude of the theft. When you are dealing with tens of millions of dollars of intellectual property being stolen and you have an individual employee involved in the larceny who is earning $20,000, he can easily be induced or seduced by $5,000 to transfer that property. Your remedy against him in terms of economic restoration is non-existent.

Chairman SPECTER. Especially where the new employer indemnifies him as you articulate in your——

Dr. DAMADIAN. So much the worse.

And I think the——

Chairman SPECTER. Let me ask you one final question, because I want to take a minute or two with Mr. Shaw.

You show Japan has a deficit——

Dr. DAMADIAN. That's an American deficit.

Chairman SPECTER. We have a deficit of $320 million, and you say that had your situation been different, that would have been a surplus of $320 million.

Dr. DAMADIAN. Or more. What I mean by that——

Chairman SPECTER. Explain how you come to $640 million. I know the MRI is a great instrument, but how do you quantify that?

Dr. DAMADIAN. No. What I am saying is that the patent, the original patent for the MRI is entirely an American invention. If our patent had been properly enforced, to which we would have been given protection from other corporations from making the same instrument, we would—America would have had the entire fruits of multibillions of dollars of this industry annually, and that—those revenues would have grossly offset that trade deficit with MRI alone. It is annually, worldwide, it's a $6 billion a year industry. Domestically it's approximately $2 or $3 billion a year, and all I am saying is that in the enforcement of my patent, America had the opportunity to capture the whole ball of wax, and lost it.

Chairman SPECTER. A $6 billion a year industry?

Dr. DAMADIAN. Oh, absolutely.

Chairman SPECTER. Mr. Shaw, What has happened to your company? You have gone forward with another company. Are you able to utilize at least to some extent the fruits of your labors there?

Mr. SHAW. No, sir. We are able to use some of the experience that we gained, and we use related software technologies that we also were responsible for inventing. But Ellery Systems is no longer with us.

Chairman SPECTER. Well, I am sorry to hear what your experiences have been, and the criminal law is the best weapon we have short of waging war on some other country. If an employee comes back, having been away, and now having breached a non-competitive agreement and suddenly the information turns up in the hands of a foreign company, a criminal prosecution is minimal there. And what we will have to explore later is what our extradition treaties are beyond the employee as to what we can do by way of getting jurisdiction over the perpetrators in the other country, to really go after the big time guys.

Dr. DAMADIAN. Well, Mr. Chairman, if I may suggest, there is another very potent weapon which I think your bill addresses, but not to be underestimated, and that is the access to the largess of our gigantic internal market is a prized plum by most of these perpetrators, and denial of access to that marketplace for the perpetrators of governments, which is what you raised earlier, I think would be very effective deterrence, because many of these multinational companies manufacture a very large line of products, which they would—whose gross revenues greatly exceed an individual product where they may be perpetrating this espionage, and would not like to lose the entire access to this massive internal market as a consequence.

Chairman SPECTER. Well, my red light is on, so I will conclude simply by noting that imposing a sanction against a foreign company from importing is something we can do perhaps a lot easier than we can get extradition on the president of a foreign corporation.

Senator Kohl.

Senator KOHL. Thank you, Mr. Chairman.

As a follow-up, I would like to ask both of you gentlemen why you think, or do you think that this piece of legislation that we are considering here will make a big difference, or a small difference, or really improve upon the problem that we have, or are we just touching the surface in a way that is not going to be very effective.

Mr. Shaw, what do you think?

Mr. SHAW. Senator, if your legislation was law 2 years ago, the outcome of the case that affected Ellery Systems would have been entirely different. Indeed, I doubt very seriously if the crime would have been committed in the first place. Given the inevitability of the kind of thing that happened to Ellery Systems, that is continuing to happen to companies across this country, in the full spectrum of technology industries that we are all engaged in, this type of legislation will provide a punitive deterrent, both to the employees of companies who may be involved, and it would certainly make it much more difficult for foreign governments or agents of foreign governments to seduce or otherwise recruit these types of——

Senator KOHL. Will you tell us why you think the existence of this law would have perhaps prevented the theft that occurred with you?

Mr. SHAW. It came to our attention over a course of 18 months, while we pursued this case just how widely spread this activity was. Even though we were aware of this kind of thing going on, the FBI had made sure in prior years, because of the nature of some of the other work that we did, continue to do, that this type of activity is widely spread.

But from talking to a number of other industry leaders—and I sit on the board of the National Information Infrastructure Test Bed Consortium and a number of other industry boards and consortia, it became clear that one of the problems that industry acknowledges is that there is no crime for stealing intellectual property from a technology company. Therefore, given that the employee or another agent recognizes that there is no crime, there will be no time spent behind this action, that, coupled with substantial financial inducements—a half a million dollars in cash is a lot of money, Senator, for a—for this technology. Knowing that you are not going to do any time behind any crime and you're going to pick up a half a million dollars for a few moments work, that's a lot of inducement for a crime.

Senator KOHL. Mr. Damadian.

Dr. DAMADIAN. Yes.

I think the other thing to keep in perspective is that I would estimate that the vast majority of this technological—critical technological information is transferred for far less than a half million dollar inducements. Much more—if you knew the gross amount, I wouldn't be surprised if many of the inducements were on the order of a few thousand dollars.

And if I were to guess, I would say that your bill, as it is crafted, would deter 80 to 90 percent of those considering such pilferages, especially when you put it together with the prospect of them having to face some inquiries from the FBI.

Senator KOHL. Well, that's very good to hear.

Mr. Shaw, can you estimate the value of the information that was stolen from you?

Mr. SHAW. Yes, sir.

In terms of actual billing records, time that was put in over a period of 2 years prior to the theft, there was in excess of a million dollars of employee time billed. There was considerably more time spent in a number of years, 7 or 8 years prior to those records that I mentioned having been spent. I don't think it is possible to estimate the value of the time spent from 5 p.m. to 5 a.m. when as many as 10 or 15 of those employees would still be there, working on that technology, because it was their's.

Senator KOHL. OK. Mr. Damadian, how much do you spend on security measures to prevent economic theft?

Dr. DAMADIAN. We have a fairly elaborate program. All of our PC's that are involved in R&D have their disk drives removed, modems disconnected, all of the schematics—no schematic can be issued without my personal signature. All of the schematics have the employee sign across the face of the schematic in large magic marker, his name, personally. We have video cameras that are

trained on all secure areas to monitor those areas continually. But in an information age, where somebody can put a CD–ROM in his pocket, or go to a computer we've overlooked and modem the information across the Internet internationally, I don't know how to control it.

Senator KOHL. OK.

What were your security measures, Mr. Shaw?

Mr. SHAW. We have—Ellery Systems had a global or globe spanning network of high end computers, networked computers. As a consequence, we had some fairly sophisticated logging procedures in place, automated software systems in place that would be—would notify us when certain files, certain file types were being transferred and where they were being transferred. Because of the very nature of our work, where we are transferring gigabytes of information hourly around the world, it took, in this case, as many as 3 or 4 days for those logs to be examined by one of the security technicians at the company to notice the crime. These are very expensive, but they are not infallible measures.

Senator KOHL. Thank you. Thank you, Mr. Chairman.

Chairman SPECTER. Thank you very much, Senator Kohl.

I would like to acknowledge the presence today of the Director of the National Counterintelligence Center, Mr. Michael Waguespack.

Can you step forward, sir.

Let me just ask one question as to your being tasked with the job of issuing the annual report on foreign industrial espionage targeted against U.S. industry. How extensive is this problem in your view?

TESTIMONY OF MICHAEL WAGUESPACK

Mr. WAGUESPACK. Well, Senator, as I think the first annual report, which we submitted to you through the President, certainly is indicative that there is a substantial threat. As Director Freeh testified earlier today, certainly there are indications that that threat is increasing. I think as he articulated, the number of cases that the FBI has initiated over the course of the last year would indicate that there is an increasing threat. More and more companies are willing to come forward with the information. So we are learning more and more about it, and certainly the more we learn about it, the more we understand that this is a serious threat and a growing threat.

Chairman SPECTER. Well, we thank you for the report, and we thank you, Mr. Damadian and Mr. Shaw, for coming in today. I think this hearing is going to give considerable impetus to have other companies come forward to specify the kinds of losses which they have had, which are just extraordinary. It is past time that action be taken with Federal legislation to combat the issue. I think you were right, Mr. Damadian, if you start talking to importers about limiting the U.S. market, this is the jewel, and nobody likes to talk to the FBI, except perhaps at one of these hearings.

Thank you all very much.

[Whereupon, at 12:40 p.m., the hearing was concluded.]

○

25–063 (122)

ISBN 0-16-052862-3