CORPORATE AND INDUSTRIAL ESPIONAGE AND THEIR EFFECTS ON AMERICAN COMPETITIVENESS

HEARING

BEFORE THE

SUBCOMMITTEE ON
INTERNATIONAL ECONOMIC POLICY AND TRADE

OF THE

COMMITTEE ON
INTERNATIONAL RELATIONS
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

SEPTEMBER 13, 2000

Serial No. 106–180

Printed for the use of the Committee on International Relations

Available via the World Wide Web: http://www.house.gov/international_relations

U.S. GOVERNMENT PRINTING OFFICE
68–684 CC WASHINGTON : 2000

COMMITTEE ON INTERNATIONAL RELATIONS

BENJAMIN A. GILMAN, New York, *Chairman*

WILLIAM F. GOODLING, Pennsylvania
JAMES A. LEACH, Iowa
HENRY J. HYDE, Illinois
DOUG BEREUTER, Nebraska
CHRISTOPHER H. SMITH, New Jersey
DAN BURTON, Indiana
ELTON GALLEGLY, California
ILEANA ROS-LEHTINEN, Florida
CASS BALLENGER, North Carolina
DANA ROHRABACHER, California
DONALD A. MANZULLO, Illinois
EDWARD R. ROYCE, California
PETER T. KING, New York
STEVEN J. CHABOT, Ohio
MARSHALL "MARK" SANFORD, South Carolina
MATT SALMON, Arizona
AMO HOUGHTON, New York
TOM CAMPBELL, California
JOHN M. McHUGH, New York
KEVIN BRADY, Texas
RICHARD BURR, North Carolina
PAUL E. GILLMOR, Ohio
GEORGE RADAVANOVICH, Califorina
JOHN COOKSEY, Louisiana
THOMAS G. TANCREDO, Colorado

SAM GEJDENSON, Connecticut
TOM LANTOS, California
HOWARD L. BERMAN, California
GARY L. ACKERMAN, New York
ENI F.H. FALEOMAVAEGA, American Samoa
DONALD M. PAYNE, New Jersey
ROBERT MENENDEZ, New Jersey
SHERROD BROWN, Ohio
CYNTHIA A. McKINNEY, Georgia
ALCEE L. HASTINGS, Florida
PAT DANNER, Missouri
EARL F. HILLIARD, Alabama
BRAD SHERMAN, California
ROBERT WEXLER, Florida
STEVEN R. ROTHMAN, New Jersey
JIM DAVIS, Florida
EARL POMEROY, North Dakota
WILLIAM D. DELAHUNT, Massachusetts
GREGORY W. MEEKS, New York
BARBARA LEE, California
JOSEPH CROWLEY, New York
JOSEPH M. HOEFFEL, Pennsylvania
[VACANCY]

RICHARD J. GARON, *Chief of Staff*
KATHLEEN BERTELSEN MOAZED, *Democratic Chief of Staff*
JOHN P. MACKEY, *Republican Investigative Counsel*

SUBCOMMITTEE ON INTERNATIONAL ECONOMIC POLICY AND TRADE

ILEANA ROS-LEHTINEN, Florida, *Chairman*

DONALD A. MANZULLO, Illinois
STEVEN J. CHABOT, Ohio
KEVIN BRADY, Texas
GEORGE RADANOVICH, California
JOHN COOKSEY, Louisiana
DOUG BEREUTER, Nebraska
DANA ROHRABACHER, California
TOM CAMPBELL, California
RICHARD BURR, North Carolina

ROBERT MENENDEZ, New Jersey
PAT DANNER, Missouri
EARL F. HILLIARD, Alabama
BRAD SHERMAN, California
STEVEN R. ROTHMAN, New Jersey
WILLIAM D. DELAHUNT, Massachusetts
JOSEPH CROWLEY, New York
JOSEPH M. HOEFFEL, Pennsylvania

MAURICIO TAMARGO, *Subcommittee Staff Director*
JODI CHRISTIANSEN, *Democratic Professional Staff Member*
YLEEM POBLETE, *Professional Staff Member*
VICTOR MALDONADO, *Staff Associate*

CONTENTS

WITNESSES

	Page
Sheila W. Horan, Deputy Assistant Director for Counter Intelligence, National Security Division, Federal Bureau of Investigation	3
Dan Swartwood, Corporate Information Security Manager, Compaq Computer Corporation	12
Scott Charney, Partner, PricewaterhouseCoopers	14
Austin J. McGuigan, Senior Partner, Rome, McGuigan, and Sabanosh, P.C	16

APPENDIX

Prepared statements:

The Honorable Ileana Ros-Lehtinen, a Representative in Congress from Florida and Chair, Subcommittee on International Economic Policy and Trade	26
Sheila W. Horan	29
Dan Swartwood	40
Scott Charney	48
Austin J. McGuigan	51

CORPORATE AND INDUSTRIAL ESPIONAGE AND THEIR EFFECTS ON AMERICAN COMPETITIVENESS

WEDNESDAY, SEPTEMBER 13, 2000

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON INTERNATIONAL ECONOMIC
POLICY AND TRADE,
COMMITTEE ON INTERNATIONAL RELATIONS,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:09 p.m. in room 2200, Rayburn House Office Building, Hon. Ileana Ros-Lehtinen (chairman of the Subcommittee) presiding.

Ms. ROS-LEHTINEN. The Subcommittee will come to order.

The past decade has brought profound changes, yet some of the characteristics of the old world order continue to live on today, with some of the darker impulses of yesteryears adapting to fit a new time and a new set of standards and requirements.

The front line is no longer the one which divides East and West, but the one defined by technological innovations. The battle lines lie in research and development. Resources designed and previously used exclusively for military intelligence gathering are now being expanded to gather intelligence on mergers, investments and other financial transactions. The generals are being replaced with CEOs, and the bottom line is not ideological, but financial.

The threat of economic and industrial espionage looms over the horizon of the business world like a gray cloud threatening a placid sea. Those who develop a competitive advantage over their rivals stand to make millions from their innovations. That profit is enough for some to seek an unearned advantage of their own by indulging in corporate espionage as a quick fix solution to their creative deficiencies and their inability to remain competitive in their field.

In a survey of Fortune 500 companies, the American Society for Industrial Security estimated that last year U.S. corporations sustained losses of more than $45 billion from the theft of trade secrets. Companies reported that on average, each had suffered 2.5 incidents of unauthorized appropriation of proprietary information. The average estimated loss per incident was calculated to be over $500,000, with most incidents occurring in the high technology and service sectors.

In another study, Pacific Northwest National Laboratory, under contract by the FBI, developed an economic loss model in an attempt to assess economic losses resulting from intellectual property

theft. This model determined that the misappropriation of intellectual property resulted in over $600 million in lost sales and the direct loss of 2,600 full-time jobs per year.

The same technology which has propelled our economy to unparalleled heights is also the mechanism which allows for those practicing corporate espionage to more easily sneak into a corporation's files, gather sensitive information and escape without a trace. However, industrial espionage is a crime which continues to be best accomplished through low tech means and is not necessarily dependent upon high tech gadgetry.

A vast majority of corporate espionage crimes do not occur in cyberspace, but rather in person, face to face. For example, key employees within a given corporation might be sought by a rival company for information or recruited by spies posing as consultants or headhunters at trade shows.

Competitors often examine a company's own internet home page, where key technical employees are often listed, and craft strategies on how to lure that employee away from that firm. This is done because information can be meaningless without the help of trained employees who understand how a particular technology is used.

A critical step was taken in 1996 with the passage of the Economic Espionage Act. Since its enactment, the U.S. Government has prosecuted 18 cases of corporate or industrial espionage, yet these crimes and the threat they pose to U.S. economic security continues to escalate.

Some would argue that this is because we are the leading target of these crimes due to our position in the global marketplace and our technological leadership. The United States produces the majority of the world's intellectual property capital, including patented inventions, copyrighted material and proprietary economic information. Factor in the incredible ingenuity and inventiveness of the American worker, and one can easily see why this problem is so pronounced in the American workplace.

Other observers contend that if the punitive portions of the Economic Espionage Act were strengthened to make it more costly for corporations and governments to engage in industrial espionage against the United States, the desired deterrent effect would be achieved. Many have raised export restrictions as a strong option for the United States to take, and have underscored the need to secure binding commitments from our allies in the Organization for Economic Cooperation and Development and other international forums.

We hope to examine these and other pertinent issues during the course of today's hearing and look forward to the recommendations of our panelists on the steps that Congress can take to help curtail the proliferation of economic espionage.

I would like to yield to the Ranking Member of our Subcommittee, Mr. Bob Menendez of New Jersey.

Mr. MENENDEZ. Thank you, Madam Chairlady. I appreciate your hearing today. This is an important subject, one that warrants and receives increasing attention. As our witnesses have pointed out in the past and will again today, opportunities to steal trade secrets are on the rise, particularly as society relies more and more on

computers and the internet for the development, storage and communication of ideas and designs.

For the purposes of this hearing, of course, we really should distinguish between legal and illegal spying or corporate intelligence, as legitimate gathering of company data is called, and as we are the International Relations Committee we must, of course, distinguish as well between domestic and foreign theft.

Only a fraction of the problem is actually foreign theft of U.S. trade secrets. According to the American Society for Industrial Security, more than three of every four thieves are employees or contractors. Another 6 percent or more are domestic competitors. Only 7 percent steal secrets on behalf of a foreign company or government. Still, this amount of foreign theft of U.S. trade secrets amounts to possibly billions of dollars annually, and ease of access to computers and internet and intranet sites will make foreign theft much easier and much more common.

I realize that much of the testimony today will focus on the problem as a whole, on the threats from employees, on the need to educate businesses about the risks and how to protect themselves, on the need to inform the public and policymakers about what is acceptable and not within the bounds of corporate intelligence, but I do hope also that we can focus to the extent possible on what exactly are the threats from abroad and how government can best work to prevent corporate espionage that will threaten the United States' competitiveness.

I know that our witnesses will make some specific recommendations for new and improved legislation, and we look forward to exploring those with you. We look forward to the responses of the Administration as to some of those and to the testimony here today.

Thank you.

Ms. ROS-LEHTINEN. Thank you so much, Mr. Menendez.

It is a pleasure to have with us our first Administration witness who will share with us her views on the effects which corporate and industrial espionage have American competitiveness. It is our pleasure to introduce Sheila Horan, Deputy Assistant Director on Counter Intelligence for the Federal Bureau of Investigation.

A special agent of the FBI since 1973, Ms. Horan has held a number of positions within the Bureau, including Assistant Special Agent in Charge for Administration in the New York office and the Associate Special Agent in Charge in Philadelphia. In 1998, Ms. Horan was transferred to her current position as Deputy Assistant Director for Counter Intelligence with the National Security Division at FBI headquarters.

We thank you, Sheila, for being here today. We will include your entire testimony for the record, and feel free to abridge your comments.

[The prepared statement of Ms. Ros-Lehtinen appears in the appendix.]

STATEMENT OF SHEILA HORAN, DEPUTY ASSISTANT DIRECTOR FOR COUNTER INTELLIGENCE, FEDERAL BUREAU OF INVESTIGATION

Ms. HORAN. Thank you very much, Madam Chairman. I am gratified to see that you are anxious and willing to engage with us

in grappling with the immense problem facing us today with regard to the protection of sensitive information, proprietary information, security, economic competitiveness and economic security in this——

Ms. ROS-LEHTINEN. Ms. Horan, if I could interrupt you?

Ms. HORAN. Yes?

Ms. ROS-LEHTINEN. I am so sorry, Mr. Burr. I should have looked back. I have these funny glasses on today. I apologize.

Mr. BURR. The gentlelady is awfully kind to stop, but I would rather hear from our witnesses. I thank the Chair.

Ms. ROS-LEHTINEN. Thank you. I am so sorry.

Ms. HORAN. Thank you, sir.

So you have my statement, and rather than regurgitating that now I will just make some points, and then we can get on to the questions if you would like.

The Attorney General essentially defines economic espionage as the unlawful or clandestine targeting and acquisition of sensitive financial, trade or economic policy information, proprietary economic information or critical technology.

In today's environment, intellectual property and economic information in general have become the most important and sought after commodity by all nations of the world. No question about it. I would say that because of our unique position in the world as a target rich nation for natural resources, intellectual property, just general overall wealth, that we are the No. 1 target in the world for economic espionage and the stealing of that information and secrets.

Why are we the most sought after commodity? The United States, that is. It is a pretty complex situation actually, but three reasons sort of come to the fore. The first is the collapse of the Soviet Union and the tremendous relief that that has brought throughout the world.

There were essentially, and not to be overly simplistic, but two large camps in the world, and various countries in the world devoted their natural resources, their personnel resources and their general overall wealth toward supporting their position either with the west or with the Soviet empire.

When the empire fell, they found themselves looking around and saying look, we have got to redefine what is our national security. It is no longer aligning ourselves with the Soviet Union or the west. It is we have to have a piece of the economic pie. We want to do this. We want to have wealth as well. So the intelligence services, as well as the governments themselves, said who has the most, and the answer is the United States has the most.

Second, allies, military allies, who were—as well as ideological allies—during that last 50 years of our history are now aggressive economic competitors. We are faced with former friends I do not want to say attacking, but certainly working against us very aggressively in order to get again a piece of the pie.

Third, rapid globalization of the world economy defines national security not so much in how many tanks you have deployed or how many soldiers you have on the field necessarily, but instead their strength is measured in terms of the nation's economic capability.

So the nations of the world, as well as our own, and President Clinton underscored this point I think back in 1991 by saying now we should realize very strongly that national security equals economic security. That is an extremely important point I think for us to keep in mind in terms of our war or our fight against economic espionage.

What are the targets? Very briefly, they come in sort of two flavors, if I could be a little bit flip there. We are still facing the threat and the attempted threat on classified military defense related national information. There is no doubt about that. There is still ongoing, and we are always battling espionage cases on that basis.

Coming out of classified information, however, and related to classified information is cutting edge technologies, dual technologies, sensitive information that may not reach the classified level and, hence, would not be subject to an espionage case, but certainly would be fodder for economic espionage cases and our inspection of those kinds of cases.

The other flavor, if you will, is the non-sensitive area and theft of our non-high tech products and services. It is very important to realize that the way we approach economic espionage investigations. It does not have to be high tech for us to take an interest in something. A trade secret can be just as valuable in many instances as more sensitive or classified information.

So that is how we approach that, and the way we approach it is through the Economic Espionage Act, which you have already indicated that is out there. Prior to 1996, there was only state laws and some civil remedies for companies and individuals and entities to pursue theft of their trade secrets or theft of their proprietary information.

In 1996, the law gave us an overarch or gave the Federal Government the ability with the Federal law to approach the theft of trade secrets offering stiffer penalties and other advantages that were not available to us and to business and industry to pursue these cases. We have prosecuted you mentioned 18. Actually up to date there are 20 in which we have successfully prosecuted over the last 4 years.

Interestingly enough, the Department of Justice or Congress actually, not the Department of Justice, was concerned that we would take this law in 1996 and profligately investigate all sorts of smaller issues and inappropriate crimes under this umbrella. I think that you can be well served and proud that in the 4-years the Bureau and the Department of Justice have carefully looked at these cases and have had what I consider a tremendous success in the 20 cases that we have prosecuted.

We are truly faced with a problem that because of the Cold War and our 50 years' involvement in that perhaps did not allow us to focus as we should have as an intelligence community, as a government, on this problem. It is not a new problem. It has been around for years and years and years, but our government was focused on the Cold War issues and realities and perhaps did not have enough time to pursue this as aggressively as we are trying to do today.

Let me stop there, Madam Chairman, and engage with you and your fellow Members any issues that you might want to pursue.

[The prepared statement of Ms. Horan appears in the appendix.]

ROS-LEHTINEN. Thank you so much for your testimony.

Mr. Burr, in order to make up for it I would like to recognize you first for the questions.

Mr. BURR. The gentlelady is awfully kind.

Let me ask you, if I can. Can you give us some type of percentage as to what you see that would be the classified part that the theft is going after versus the non-classified?

Ms. HORAN. Let me answer that, Mr. Burr, by saying that there are two provisions in the Economic Espionage Act. One is 1831, which deals with economic espionage attempted and conducted by a foreign entity, that is to say a foreign intelligence service, a foreign government, a foreign organization linked to the actual government.

The other provision is 1832, which, generally speaking, you could characterize as a theft of trade secrets and would be aligned with possibly white collar crime violations, theft of essentially trade secrets, as I said.

The vast majority—well, of the 20 prosecutions that I mentioned to the Chairwoman that we have pursued, none of them fall in the former category of the foreign power based or supported category. All 20 have been in the 1832, which is the trade secrets.

In terms of how many cases, actual cases we are pursuing that fall into the two camps, I would say that the percentage is at this stage highly weighted in the trade secrets or the non-classified versus the classified, although we have a number, and I would prefer not to get into actual numbers in this open forum, but we do have a goodly number in the other category, the foreign based category.

Mr. BURR. And is there any dollar amount that the Bureau has put on the current economic espionage that exists for the U.S. economy?

Ms. HORAN. We have not. As the Madam Chairperson has mentioned, there were two, at least two, studies conducted. ASIS did one and PNNL conducted another one in which they projected. The PNNL case projected out of an actual trade secret prosecuted or trade secret case. They projected out even to tax loss, job loss, as well as monetary loss to the company itself.

While that is illustrative to us, as is the American Society for Industrial Security study, both of them are very illustrative of what the actual loss is and magnificent essentially. It is huge.

Mr. BURR. I thank you and yield back to the Chairman.

Ms. ROS-LEHTINEN. Thank you so much.

Ms. HORAN. OK.

Ms. ROS-LEHTINEN. Thank you.

Mr. Menendez. I know we have a vote.

Mr. MENENDEZ. I have one question or two actually. Maybe just by joining together you can answer them together.

Ms. HORAN. Sure.

Mr. MENENDEZ. I understand there are, you said, about 20 cases or so that have been prosecuted under the EEA. I understand that this is in part due to an agreement or an understanding or a pledge by the Attorney General not to prosecute cases or not to have the government pursue charges without first having obtained

the Attorney General's personal approval to proceed and that there are 800 cases now being considered for prosecution. Is that a correct number, and would we expect the amount of prosecutions to go up after the 5-year waiting period?

No. 2, is the suggestion that closing—from some of the other witnesses we will hear about closing the loophole that prevents prosecution for theft of their product before it is placed into interstate or foreign commerce and the creation of a private cause of action under the EEA, are those items that the Department has considered or has——

Ms. HORAN. I am not aware of the Department's view on the latter issue, but on the former issue——

Mr. MENENDEZ. If you would have the Department give us a written response to that?

Ms. HORAN. Yes, certainly I would. By all means, Mr. Menendez.

Your first question, though, would we expect an up tick, so to speak, in the number of prosecutions, and also you asked about the figure 800 and whether that is accurate. I would say that is not accurate at this time. We have about as of today, because I checked thinking you might want to know this. We have about 400 cases open today.

Mr. MENENDEZ. Four hundred?

Ms. HORAN. Four hundred. Because of the education efforts that we are engaging in and trying to get the word out about this, you must understand that industry and business are somewhat loathe and reticent in engaging with us, but the more they hear about the cases, the more they see the results, we anticipate that those cases are going to raise exponentially and in fact have raised over the years heretofore. Have increased I should say, so, yes, definitely.

Mr. MENENDEZ. I really look forward to the Department's response.

Ms. ROS-LEHTINEN. Thank you, and I am pleased to recognize Mr. Manzullo, who will take over for us. Thank you.

Mr. MANZULLO [presiding]. This is like musical chairs.

Ms. ROS-LEHTINEN. Thank you.

Mr. MANZULLO. Thank you.

I get to ask you the questions, yet I have not even heard your testimony.

Ms. HORAN. Well, I will be happy to hand it to you right now.

Mr. MANZULLO. I have it right here. Forgive me if I ask this question——

Ms. HORAN. That is quite all right.

Mr. MANZULLO. What is the line beyond which inquiry or gathering information becomes a violation of the Economic Espionage Act?

Ms. HORAN. Let me try and answer that question this way. There are a number of ways that we look at and approach economic espionage in the FBI and intelligence community wide. We are not doing this ourselves. We are enjoined with the Department of Defense, the Central Intelligence Agency, Commerce, Customs, etc. This is not an FBI unilateral responsibility, but we sort of coordinate it.

One of the main ways we do that is utilizing the Economic Espionage Act of 1996, which I think is what you are referring to. We also have a responsibility under our counterintelligence mandate

and apart from any criminal mandate to gather information and collect and disseminate information with regard to foreign targeting of our infrastructure, of our government, of our business academia, business and industry, etc., with the idea that using investigative steps, which I probably will not get into here, but trying to stem that, avoid it, prevent it and get around it, stop it before it actually happens.

It is a huge analytical effort, and that is one whole aspect that we probably will not talk about today, but that is one area that we have a lot of effort in.

With respect to when does an individual or a member of a foreign government step over the line, I would have to say that it is a case by case situation. You have to really look at the circumstance, the totality of circumstances involved in each situation, but what the law does not want us to do, and this is part of that line, is to say to diplomats and legitimate government or personal envoys from abroad or from within our own country that they cannot collect open source information, economic information that is out there on whether it be the internet, whether it be libraries, wherever it lies.

So we are not trying to impact or stop that kind of activity. Where we would like to have an impact and where many of the 20 cases that have been prosecuted so far have led us is where a foreign or a domestic, a foreign or a non-foreign, entity is attempting to rip away some element of our economic competitiveness, generally speaking, in the business world here, in the business industry.

Mr. MANZULLO. Can you——

Ms. HORAN. I am sorry.

Mr. MANZULLO. In the context of that answer, can you give us an example of someone who you have prosecuted——

Ms. HORAN. Sure.

Mr. MANZULLO [continuing]. That is a matter of open record?

Ms. HORAN. Sure.

Mr. MANZULLO. Thank you.

Ms. HORAN. As I say, there are 20. I will—probably the most widely known one and one that you may be aware of is the Bristol-Myers Squibb Taxol case, which was resolved a couple of years ago, Taxol being a very, very popular cancer fighting drug, and it was the subject of theft from a Taiwanese company who sent employees here to attempt to steal that. We prevented that thankfully. They went through the court process and arrests were made, and it was prosecuted successfully.

That is one of them, but let me, I think, to give you an idea, I will just quickly tell you some of the—and this goes to a comment that I made that it need not—our prosecutions and our interests need not be only in cutting edge, dual use technology, sensitive, proprietary information, but can be non-high tech. I do not think you were here for this part; non-high tech issues, trade secret issues that we are very interested in, too.

For instance, the Joy Mining Machining Company in Pittsburgh, PA. Technical coal mining equipment was being targeted. Deloitte & Touche was the victim of one case, and a proprietary software program was targeted. Gillette Company was the victim in another case. A new shaving system was the target.

Mr. MANZULLO. How many ways——

Ms. HORAN. On and on.

Mr. MANZULLO [continuing]. Can you use to cut whiskers?

Ms. HORAN. Well, they evidently had a new one. I do not know what it was.

Mr. MANZULLO. I do not want to use the word watchdog, but obviously you got involved at a point where the company owning the patent or the trade secret had some kind of an indication that somebody was trying to steal it?

Ms. HORAN. That is correct.

Mr. MANZULLO. That would be the normal way?

Ms. HORAN. It can be two ways. Either they detect this, which is frequently the case, or we get information that something is amiss.

This brings up an interesting point. I am glad you made that point that companies are sometimes reluctant to come to the Federal Government and the Federal Bureau of Investigation for these kinds of investigations, No. 1, because they are largely ignorant of how we do them, and we are trying to successfully overcome that by an education program, but they do not want their trade secrets to be aired. They do not want their shareholders to know there are problems in the company. These kinds of bottom line issues are very difficult to overcome when a company comes and finds out information like this.

Just this very morning we were in contact with one of the major oil companies in the United States who phoned in and wanted—the director of security phoned in and said look, we found that we have information that someone is trying to steal XYZ from us, and I am going to make a presentation—I am the director of security—to the CEO about whether we should involve the FBI or not, so these kinds of problems are plaguing us right now because it is a new law and people do not know, but we think we will overcome this as time goes on hopefully with some good, high level, highly publicized deterrent factors.

Mr. MANZULLO. This is a good segue to these questions that the Chairlady had circled, which I will ask now.

One of the witnesses on the second panel will state that since the value of trade secrets is not well established, safeguarding efforts are often given lower priority when limited resources are allocated. The question here is do you agree with this assessment?

Is there a wide gap between the value of lost assets and resources allocated to investigation, enforcement, prosecution of economic espionage? How do you establish a clear value for the assets? This goes right to the heart of your work at the FBI, does it not?

Ms. HORAN. It does.

Mr. MANZULLO. It is obviously high priority for you because this is your mission, is it not?

Ms. HORAN. Pardon me, please. Yes, it is a high priority for us and will continue to be one I think in the coming years because of the escalating costs that it is——

Mr. MANZULLO. And you focus your career almost entirely on this, is that correct, in the FBI?

Ms. HORAN. Me myself?

Mr. MANZULLO. Yes.

Ms. HORAN. Personally? It is one of the responsibilities. I am in charge of counterintelligence for the Bureau, so this would be one aspect of it——

Mr. MANZULLO. OK.

Ms. HORAN [continuing]. But certainly one growing and very important one, but I would say to you in answer to your comment there that if you go out to major corporations in the United States and look at their security departments, you are going to find that generally, generally speaking, the heads of the security departments are not first line executive, and by that I mean it is not a particular company's first mission, security.

Mr. MANZULLO. They are not trained in it?

Ms. HORAN. Well, Delta Airlines take for instance. Their mission is to fly planes. The director of security at Delta Airlines, and this is multiplied across the country, is a drain on company resources because that person wants to say, "listen, in order to prevent bombs from going on the plane, in order to prevent luggage from being stolen, in order to prevent our executives from being kidnapped, this is what I need. This is how much money I need."

They are not, generally speaking, welcomed, euphemistically speaking. Not literally, but they are not always the most favorite person at the party, so to speak, so again it is an education process.

Mr. MANZULLO. Do you mean within the company?

Ms. HORAN. Exactly right, so resources, and I think this is what you were getting at. Resources in private industry devoted to security issues are much less than probably they should be in many instances.

Mr. MANZULLO. I do not know if this question was aimed at the belief that there is a low priority within the FBI or within the company itself. That is why I said——

Ms. HORAN. Not a low priority with us.

Mr. MANZULLO [continuing]. Based upon your testimony——

Ms. HORAN. No.

Mr. MANZULLO [continuing]. I do not think it is a low priority.

Ms. HORAN. Not at all, no, but my response was to private industry.

Mr. MANZULLO. Do you think the big problem is that there is so much snooping going on that people just cannot fathom the sophisticated means of doing it and the extent to which people would actually steal the product, their patent or something like that?

Ms. HORAN. Yes. I do not think people expect it.

Mr. MANZULLO. And they get blindsided?

Ms. HORAN. That is exactly right. Some of the methods used to do this are fairly innocuous and not geared toward raising anyone's hackles unless you happen to be a security person or an investigator or something who is well schooled in this spotting and assessing, for instance, an individual in a company who might be near to a particular technology, getting to know that person, building up a relationship. These are some of the methods that are used.

Additionally, what you see more and more are unsolicited requests to businesses from—either domestically or internationally in which hundreds of thousands of E-mails are sent around the world asking for particular information from, you know, someone who is interested in getting it.

It is an information gathering technique that a foreign entity can use to just send to all our countries—pardon me. All companies that deal with a particular technology that they are involved in. So they send out 1,000 E-mails. They may get back two, but they are getting back information very cheaply.

Mr. MANZULLO. Do you mean just enough to know that somebody has something there that they want?

Ms. HORAN. Oh, yes. Yes. Visits to U.S. facilities, the visitor programs, DOD, DOE, NASA. All these government entities and quasi government entities have hundreds of thousands of visitors who come to their doors each year on legitimate business, but they are also collectors, and they bring that back to their home country.

Is that something that we should be concerned about? I would say absolutely.

Mr. MANZULLO. Los Alamos?

Ms. HORAN. Los Alamos is an extremely good example.

Mr. MANZULLO. Do you or people that work under you at the FBI put on seminars for companies on——

Ms. HORAN. Yes.

Mr. MANZULLO. Do you do seminars like that? The biggest city in the congressional district I represent has over 1,500 industries.

Ms. HORAN. What is that city, sir?

Mr. MANZULLO. Rockford, IL.

Ms. HORAN. Oh, yes.

Mr. MANZULLO. It serves some aerospace fasteners. Of course, it is anything that is kept secret, so I am sitting here thinking that perhaps you or somebody might be interested in having a seminar on how to keep your secrets from being stolen.

Ms. HORAN. Well, our Chicago field office would have what is called, as all field offices have, an answer program.

Mr. MANZULLO. OK. I really appreciate your coming here. I did not hear your testimony, and I am sorry, but I will read that.

We will be in contact with your Chicago office to see if the chambers perhaps would have, even if it is a half dozen industries. Would that be sufficient to have an agent come out?

Ms. HORAN. One industry would be enough.

Mr. MANZULLO. One industry?

Ms. HORAN. We do them to 1 or 200. It does not matter.

Mr. MANZULLO. Fine. Thank you for coming.

Ms. HORAN. You are very welcome, sir.

Mr. MANZULLO. I really appreciate it. I am sorry about the interruption with the bells, but——

Ms. HORAN. Not at all. Very understandable.

Mr. MANZULLO [continuing]. We live by this. Thanks again.

Ms. HORAN. Thank you for your attention.

Mr. MANZULLO. If we could impanel the second panel? If we could impanel the second panel before the bell starts again, and I guess it is obvious that they are not interested in televising your testimony, so I hope you do not feel too badly about that.

To complement the expertise of our first witness, we would like to introduce three gentlemen who not only understand this issue, but have dedicated a significant amount of their professional lives to dealing with this problem.

First, Dan Swartwood, corporate information security manager with Compaq Computer Corporation and primary author of "Trends in Intellectual Property Loss Survey Report." Dan is a retired U.S. Army counterintelligence officer and contributing consultant to an independent assessment of the White House security program for U.S. Secret Service.

He is a 14-year member of the American Society for Industrial Security, an 8-year member of a standing committee on safeguarding proprietary information and an avid reader of James Bond novels.

I threw that in. Next, I would like to introduce Scott Charney, a partner with PricewaterhouseCoopers. Scott is a former chief of the Computer Crime and Intellectual Property Section, Criminal Division, at the Department of Justice. Under his watch, his division investigated and prosecuted cases of national and international computer hacking, cases of economic espionage and violations of Federal criminal copyright and trademark laws.

A former U.S. Attorney and Assistant District Attorney, Scott is a published author who has written widely on the subject of protection of proprietary information.

Finally, I would like to introduce Mr. Austin McGuigan, a senior partner—is that correct?

Mr. MCGUIGAN. Correct, sir.

Mr. MANZULLO. That is an Irish name like Manzullo.

A senior partner at Rome, McGuigan and Sabanosh. He is a former Chief State's Attorney for the State of Connecticut, as well as a former adjunct professor at the University of New Haven. He is the co-author of a number of articles, including "How to Use the Economic Espionage Act to Protect Your Corporate Assets."

Well, this is pretty impressive. Dan, we will start with you. I am going to put on a 5-minute clock here and try to stick to it a little bit generally.

Mr. SWARTWOOD. I will make every effort.

Mr. MANZULLO. This is pretty sophisticated. I do not know if I can operate it.

OK. Go ahead.

STATEMENT OF DAN SWARTWOOD, CORPORATE INFORMATION SECURITY MANAGER, COMPAQ COMPUTER CORPORATION, AND CO-AUTHOR OF TRENDS IN INTELLECTUAL PROPERTY LOSS SURVEY REPORT

Mr. SWARTWOOD. Mr. Chairman, I want to thank you for the opportunity to discuss a topic that often is addressed only as a subplot in movies and occasional sensational headlines.

Mr. MANZULLO. And James Bond novels.

Mr. SWARTWOOD. That topic is economic espionage and its impact on American competitiveness.

For over 20 years, I have worked in a variety of government and civilian positions that have helped qualify me to discuss this topic. I have also been actively involved, as mentioned, in the American Society for Industrial Security international survey efforts to assess the impact of intellectual property loss for almost 10 years.

These surveys have continued to indicate that the issue of intellectual property loss is growing in both scope and impact. As men-

tioned, the 1999 survey mentioned that direct revenue losses were estimated to be as high as $45 billion and there were almost 1,000 incidents of loss reported by 45 companies alone.

For the last 5 years I have been the corporate information security manager at Compaq Computer, and during that time Compaq has grown into the 20th largest American corporation and 75th largest in the world. Compaq's work force globally exceeds 100,000 people, and we, along with other major corporations, face the challenge of information loss.

I mentioned earlier that this topic tends to make the headlines. Unfortunately, there was just a major incident this week. On Monday, it was widely reported that part of the Western Union website had been cracked, and 15,000 users' credit card information had been stolen. From my perspective, the interesting aspect is how this theft occurred.

It was reported that the site administrators, while conducting routine maintenance, had removed security measures protecting the site. This is anecdotal, but does support the premise discussed in my prepared statement, which is the majority of corporate information loss occurred because of one of three causes.

One, a lack of training for and mistakes made by authorized members of your work force. Two, the failure on the part of administrators to implement and maintain security measures, and, three, disgruntled and/or disaffected individuals working in your corporation. These issues can cause up to 85 percent of all corporate information loss.

A primary consideration determining how this issue is addressed in any corporation is the priority that senior management gives it. In any corporation, there are a myriad of competing priorities on a constant basis. Security issues tend to be addressed as a reaction to unfortunate events. The lack of adequate security and training resources can create an environment where the question is not if losses will occur. The question is when they will occur.

The surveys indicate that less than 3 percent of all IT and security dollars are spent protecting or safeguarding electronic or hard copy proprietary information. The vast majority of these dollars are spent on physical and electronic measures designed to keep outsiders from penetrating corporate spaces or networks. These are absolutely essential measures in any corporation, but it must be noted, however, that they do little to protect information from either the untrained or disgruntled insider.

Few American corporations have the resources to deal with economic espionage sponsored by either nations or foreign corporations. The Federal Bureau of Investigation and Justice Department are actively building a capability to investigate such activities, and we welcome the interest and efforts they have made to address economic and industrial espionage.

Corporate espionage, defined as outsiders penetrating corporate offices or networks, does occur and can be very damaging, but because of my experience and results of the four nationwide surveys on intellectual property loss I have been a part of, I feel that it is an issue to be addressed, but is not the primary concern of corporate America.

Because the threat to business information is not primarily foreign or caused by outsiders does not make it less real or less destructive. When a corporation is denied the full benefit of their trade secret or innovations, their business suffers, and our economy is weakened.

For the last 4 years, the Federal Government has been instrumental in engaging corporate America on the issue of infrastructure protection. These efforts are designed to protect information and networks of several critical infrastructure industries. A similar engagement addressing the larger issue of intellectual property loss might cause similar improvements in how corporations view this issue and improve our competitiveness in the global marketplace.

I want to thank you for the opportunity to address you today and would be pleased to answer any questions you might have after the speakers are done.

[The prepared statement of Mr. Swartwood appears in the appendix.]

Ms. ROS-LEHTINEN [presiding]. Thank you so much.

Mr. Charney.

STATEMENT OF SCOTT CHARNEY, PARTNER, PRICEWATERHOUSECOOPERS

Mr. CHARNEY. Thank you, Madam Chairperson. Being mindful of Mr. Menendez's comments that you have our written testimony and we should feel a little bit free to deviate, I am going to do just that.

In my career I have now been both on the government side at the Justice Department responsible for economic espionage, and now at PricewaterhouseCoopers I have clients that want economic espionage or hacking cases investigated.

Building on what was said before when the FBI was present, there is certainly a reluctance by some industry members to go to law enforcement. That has to do with several reasons, but the biggest one I see is that for a private victim if they go to the government they lose control over the case.

That is, as a private company that is being victimized they can control the investigation, decide how many resources to put toward it and call it quits if they choose to do so, whereas when you report it to law enforcement then the subpoenas come and other kinds of compulsory process, and you have to go forward. Most companies do not want to lose that control.

Having said that, I also want to highlight a few other points. I mean, it is absolutely clear that digital information is great property of value in the information age. I remember many years ago, as far back as 1992, a reporter was asking Europeans about the fall of the Soviet Union and what it meant that the United States was the world's sole superpower.

The response of most Europeans was in the new economy it is not military power, but economic power that is going to rule, and so if Willy Sutton says I go to banks because that is where the money is, then competitors are going to say we are going to computers because that is where the digital resource is.

If you look at the surveys that have come out that have been referenced in almost all the testimony, both the American Society for

Industrial Security [ASIS] and surveys by the Computer Security Institute, it is clear that the losses are mounting. The number of cases is increasing.

In the Computer Security Institute survey, for example, about 20 percent of the respondents out of 585 said that they were victims of trade secret information theft, and in terms of sheer dollar losses the survey found that the most serious losses from all the types of criminal activity listed from hacking to other kinds of abuse, the theft of trade secret information was the most expensive crime for U.S. businesses with 66 respondents reporting over $66 million in losses.

I would point out, too, that these surveys probably represent only the tip of the iceberg because most computer crime is neither detected nor reported, so to the extent that people are stealing data from computer systems that is valuable, it is probably not detected.

The reason for that is the nature of electronic theft. If I steal your car you know because it is gone, but if I steal your customer list or a design plan, you still have it and so unless you have detected that abuse you will not know that I have it, and you will remain comfortable.

To show just how bad that is, one of the difficulties has always been that when you have a supposition, such as most computer crimes are neither detected nor reported, how do you prove what you do not know? The answer is you do a controlled study.

The Defense Department did just that. They attacked 38,000 of their own machines. They penetrated security 24,700 times or 65 percent. Then they went to the system administrators and said OK, how many intrusions have you detected, and their answer was 988, only 4 percent. Then they went to DISA, the Defense Information Systems Agency, and said how many reports have you gotten, and the answer was 267 or 27 percent, so it is absolutely clear that most of these crimes are probably not detected in the first instance, and then they are not reported to anyone.

I would like to conclude by focusing particularly on the international aspects of this problem, and I think that there are some critical questions that the committee needs to think about when thinking about international economic espionage in particular. The first is what actually constitutes international espionage in the new world order. Is Chrysler an American company or a foreign company?

With all the globalization of businesses, to the extent laws and governments are concerned, as rightly they should be, about allegiances and whether this is foreign or domestic, I think that line is getting increasingly blurry. It is hard to tell. That is one problem.

The second problem is with the growth of the internet, particularly with now approximately 165 countries connected, it is going to be increasingly difficult to identify the perpetrators of these crimes. The reason for that is the internet has global connectivity. Hackers have shown the ability to weave between countries to hide their tracks.

In addition to that, there is no authentication or traceability on the internet, which means if you know your machines are being at-

tacked and people are taking sensitive data, it is extremely, extremely hard to find the source.

[The prepared statement of Mr. Charney appears in the appendix.]

Ms. ROS-LEHTINEN. Thank you, Mr. Charney.

Mr. McGuigan.

Mr. MCGUIGAN. McGuigan.

Ms. ROS-LEHTINEN. McGuigan. Close enough.

Mr. MCGUIGAN. Thank you, Madam Chairperson. McGuigan.

Ms. ROS-LEHTINEN. All right. All right.

Mr. MCGUIGAN. Thank you, Madam Chairperson.

Ms. ROS-LEHTINEN. Congresswoman Johnson and Congressman Shays send their best to you. I saw them there on the Floor. Actually, they asked me to ask you really hard questions.

Mr. MCGUIGAN. I understand at least from Congressman Shays why he would say that.

STATEMENT OF AUSTIN J. McGUIGAN, SENIOR PARTNER, ROME, McGUIGAN AND SABANOSH, P.C. AND CO-AUTHOR OF HOW TO USE THE ECONOMIC ESPIONAGE ACT TO PROTECT YOUR CORPORATE ASSETS

Mr. MCGUIGAN. A little bit about my background. I was the chief prosecutor in Connecticut from 1977 to 1985. For 4 years I was chief of the organized crime task force, and prior to that I had 3 years as a special agent in military intelligence.

For the last 11 years, I have been a plaintiff in many uniform trade secret actions throughout the United States, at least eight or nine states, so I come from this both as a government prosecutor and as an attorney who is prosecuting the cases.

I have written a number of articles about the Economic Espionage Act. I assume that everybody agrees that America's technological prowess is its real capital and that the reason for federalizing this area of criminal activity was that we needed that type of protection and expected results.

I would suggest to the Committee that there has been a disquieting dichotomy between the numbers that have been provided on estimated losses, $45 billion in 1999, $24 billion in another study, and I have cited these studies from time to time in the absence of cases.

Twenty cases, I think only nine of which resulted in any incarceration, not significant fines, not a single case under 1831 which deals with foreign entities, and truly if you call it the Economic Espionage Act it seemed it was in the first instance directed at foreign espionage.

There is not a single case that has been developed that deals with foreign espionage of all the 20 cases that are cited, one of which I believe was dismissed, so that when one looks at the record against the alleged losses, one must ask why? What is going on? Of course, the reasons are people are learning how to do these cases, etc.

Understandably, the Attorney General agreed to limit the number of cases to 50 in the first 5 years, but at this point it does not look like they are going to challenge the agreed upon limitation so that the number of cases reflects and the types of cases that have

been taken reflects that so far whatever the allocation of resources, and I do not know what the government has allocated for resources under the Economic Espionage Act, but it does not seem to be returning the kind of bang for the buck that one might expect.

As normally not a fan of the federalization of criminal law, recognizing as a former chief state prosecutor that many of the federalizations of crimes does not exactly enhance the law enforcement activities, but, in any event, this law I felt was a law that was needed.

It was needed because this was truly a national/ international problem, but I could say this. I would doubt there is any significant deterrent effect that has come out of the passage of this Act in the last 4 years. The number of cases simply would not augur that people are living in fear of being caught stealing trade secrets.

I have suggested in the material prepared for the Committee that at this point it would be something to seriously consider creating a private cause of action for individuals and companies under the Economic Espionage Act. The Uniform Trade Secret Act is presently in force in 38 states, and I believe that almost every state has common law trade secret, which would be equivalent to the Uniform Trade Secret Act, so there are trade secret causes of action in all the states.

The question is why federalize? Federalizing would direct court power in three areas in which it is needed. One is in the enforcement of injunctions. Let me explain, having had a number of these cases. If one is to get an injunction in say the State of Connecticut against an individual who has misappropriated trade secrets and that individual moves to Montana, enforcing that injunction in Montana is not as simple as one would think so that we have to discuss with companies the fact that unless we are lucky enough to have diversity, which allows us to have Federal jurisdiction, when we have injunctive power of the Court we may have problems getting enforcement in a foreign jurisdiction.

Second, I think it would provide for much easier discovery, and discovery in uniform trade secret cases, and I take economic espionage cases through investigation, is absolutely essential, so I would suggest that for that reason a Federal cause of action is warranted.

The third is executing of judgments, execution of judgments when people leave states. Although we have uniform execution, a judgment is simply not that simple. If one is trying to seize assets, once one has a Federal judgment they are in much better shape in trying to enforce it.

The fourth reason. I would suggest that when and if someone considers a cause of action that they consider having some type of pre-suit discovery orders. In other words, one of the problems in developing these cases, while one realizes in a company that the technology has been taken to a different company because they have developed something and show no pattern of having worked on it, one is not able to file an action based on the fact that they must have stolen it, so I would suggest that similar to the Copyright Act, and I have put it in my prepared remarks, that you consider some type of pre-suit discovery.

The conclusion is that given the paucity of prosecutions that you have, that while criminalization of economic espionage may have

provided some merit, the real battle is going to have to be fought by the people who are losing technology. The people who are suffering the losses are going to have to finance the war through private causes of action, and that, I suggest, would give us better deterrent effect and better protect America's technological prowess.

Thank you.

[The prepared statement of Mr. McGuigan appears in the appendix.]

Ms. ROS-LEHTINEN. Thank you. Those are very good recommendations.

Following up on improvements that we could make to the Economic Espionage Act, and I would like to ask all three panelists. The Act allows for a protective order preserving the confidentiality of a trade secret only if the prosecution requests it.

Does this afford, do you believe, sufficient protection against disclosure during legal proceedings? How would you propose that this section of the law be improved?

Mr. MCGUIGAN. Well, I would say, and it was pointed out, that companies are afraid they lose control over cases when they have the government prosecuting a case and are afraid that their trade secret will be disclosed in the case itself so that they may in effect win the battle and lose the war.

I would suggest that the law be amended so that companies—the government is required to seek the input of the company, and if a company is forced to give up the very thing for which it was trying in the first instance to protect in order to proceed with the prosecution, it should have a say in having the prosecution stopped, similar to when the government decides that giving up an intelligence informant, they do not wish to go further with the case.

Ms. ROS-LEHTINEN. Thank you.

Mr. Charney.

Mr. MCGUIGAN. I believe Mr. Charney had also——

Mr. CHARNEY. Yes. From my days as chief of the computer crime section, we grappled with this problem. You have to look at this a bit logically, though.

If the trade secret has already been stolen, the defendant has it. If the trade secret has not been stolen or has been stolen and not yet used as far as you can tell and you want to prohibit its introduction in court, there is a problem with the sixth amendment because under the right of confrontation and the right to challenge the government's evidence, he has a right to challenge the trade secret.

I will tell you that we had a case where we charged attempted theft of a trade secret. The defense asked for the trade secret, and we took it up, and we won on the theory that since the defendant was only charged with attempt, whether it was actually a trade secret was irrelevant, and, therefore, there was no need to disclose it.

The Appellate Court agreed and so we did not have to disclose it, but I would just caution the Subcommittee that if you are looking at that issue, remember that to some extent the defendant has a right to see what he has been accused of stealing for purposes of litigating for his defense.

Ms. ROS-LEHTINEN. Thank you.

Do you have anything to add? Thank you, Mr. Swartwood.

Mr. SWARTWOOD. I would comment that as the only person on this panel that actually works in a corporation, this is a very difficult issue. Often not only is it very difficult to make a determination that you have lost something, but then after you have made that determination or you feel you are comfortable that that has occurred, getting that information pushed up into the management of the organization and having a reaction, a positive reaction to that, is also somewhat problematic.

It is very difficult with all the concerns that major corporations have unless you are talking about some absolutely seminal piece of information or something that is considered so super critical. It is very difficult sometimes to get any mind space with the senior management to address these issues in any constructive way.

Ms. ROS-LEHTINEN. Thank you.

I wanted to ask about the territorial scope of the law relating to conduct occurring outside of the United States. Some suggest that there are problems with it. They suggest that the measure ought to be whether the espionage act committed overseas had a substantial effect within the United States.

Would you disagree or agree with that recommendation, and how would you define substantial effect?

Mr. CHARNEY. I think it is a difficult issue. The law already has some extra territorial provisions, as you know, and also when there is any conduct in the United States you get venue in the United States and so I guess my question would be are we looking at cases, for example, where a foreign company steals a secret in that country, but it somehow has an impact upon the United States.

I think if the United States were to exercise jurisdiction in those kinds of cases we would probably get resistance from foreign states about the reach of our law—if that is the scenario we are thinking about.

If, for example, a French company took data from IBM in France and because IBM is an American company we said well, that has an impact on IBM's corporate profits and earnings, I think we would get resistance. That is just my sense.

Ms. ROS-LEHTINEN. Austin.

Mr. MCGUIGAN. I do not know whose proposition this is a problem because I know of no case under 1831 that has even been attempted, and I cannot comment on whether or not there is a stumbling block because I simply do not see it as a stumbling block, and I have not seen a case where someone has planned out how it could become a stumbling block. I do not know what testimony there is to that effect. I do not know.

Ms. ROS-LEHTINEN. OK. Does the prospect of litigation, the threat of litigation or prosecution serve as a true deterrent for corporate spies? Are the fines that are levied under this Act, the Economic Espionage Act, a true deterrent? How can industrial espionage be made less appealing? Do you think more prosecution or heavier fines would serve as deterrents?

For example, should violator companies be sanctioned internationally whereby they cannot reap any benefits from the stolen information? Should the United States impose duties on products

from such companies or impose other import or export restrictions? What steps can be taken?

Mr. MCGUIGAN. The fine so far, and I hate to keep taking the table. The fine so far is simply in looking through I provided a table of all the cases.

Ms. ROS-LEHTINEN. Yes. We have it. Thank you.

Mr. MCGUIGAN. Simply no one could suggest that the types of fines that have been proposed could act as a deterrent——

Ms. ROS-LEHTINEN. Correct.

Mr. MCGUIGAN [continuing]. If the problem is $45 billion. It is simply not—it does not make any sense.

The only large fine is really a restitution I believe that is in the Gillette case where the gentleman sold, I believe, the new design for the Mach III razor before it came out. I believe it has something to do with that, but that is the only large one, and that is really a restitution so there does not seem to be any fines.

I would think that the threat of incarceration is more serious for corporations than money, and putting individuals in jail is the best deterrent.

Mr. MANZULLO. Yes, but they do not give you razors in jail.

Mr. MCGUIGAN. I understand that, but I think that——

Ms. ROS-LEHTINEN. Not the Mach III anyway.

Mr. MCGUIGAN [continuing]. Incarceration is a much better deterrent. For foreign companies obviously, fines are going to have to be more seriously considered, substantial ones, because incarceration is not real.

Ms. ROS-LEHTINEN. Thank you.

Mr. Swartwood.

Mr. SWARTWOOD. I think another consideration is that it would be difficult I think to try to prove that something was taken with the full knowledge and agreement of say the CEO of any major corporation.

My experience in information loss indicates that even the perpetrators of such crimes for the most part are acting as individuals and not acting necessarily at the behest of another corporation. They are doing it for their own personal reasons. They are doing it for either personal gain or for some type of retribution, etc., and once again I am talking mostly on the insiders.

In external situations, my feeling is that even when corporations, if they were involved, it would be at a level of the corporation that would not necessarily be considered corporate. I mean, you might have someone in a division trying to get a short-term gain in an area, and so, I mean, I think proving that it would be a corporate level issue could be very difficult, especially in a criminal venue.

Ms. ROS-LEHTINEN. Yes?

Mr. MCGUIGAN. I think my experience has been the opposite. In many of the cases I have taken, upper management has been involved in the misappropriation, and it has been my experience in the criminal law that when one prosecutes low level individuals they are able to get those individuals to give up the names of the people otherwise involved.

So absent again incarceration and seriously doing that, I do not see how you are going to get to the bottom of who in the company is involved.

Ms. ROS-LEHTINEN. Thank you.

Mr. Manzullo.

Mr. MANZULLO. This is very fascinating. I see two roads here. Maybe I am wrong, and you can correct me— one is an inference that says because there have been only 18 prosecutions, the FBI or Department of Justice is not sufficiently and aggressively prosecuting these types of cases. Then, on the other hand there is this natural reticence of the companies. They would rather take the hit than give a Federal agent the opportunity to take a peek at the secret.

The testimony of the Assistant Director was pretty obvious that they have to struggle with companies. She said she would put on a seminar for one company just to be able to peak their level of inquiry that the FBI is indeed interested.

Did you want to comment on that, Mr. McGuigan, because you seem to draw the——

Mr. MCGUIGAN. We in Connecticut have incarcerated at state court individuals. There are no Federal prosecutions in Connecticut, but have had the local gendarmerie prosecute individuals and actually incarcerate individuals for misappropriation of propriety drawings from one of our companies.

I think that the reasons for the dichotomy I think need to be explored between the losses and the lack of cases, but, second, I think that it should be longer incarceration because summarily dealing with some people is an object lesson for others.

What I am saying is that when you have a case I think you have to prosecute it very, very vigorously, and you have to—when you get substantial time, you will find out who else is involved, and that can have a salutary effect on a number of other individuals contemplating similar conduct.

Mr. MANZULLO. Yes?

Mr. CHARNEY. I would just like to build on this question a moment because when I was chief of the computer crime section, I can tell you that prosecutors salivate over cases like these.

You know, the first case out of the box was the Four Pillars case, which went to trial. We convicted the president of a corporation from Taiwan for stealing secrets from Avery Dennison. These are good cases with sex appeal. That is not the problem.

If you look at the Computer Security Institute's surveys, however, they have done surveys on computer crime from 1996 to the year 2000, and in the year 2000 survey what they said was one of the most remarkable statistics on computer crime—not just trade secrets, but computer crime—was the rapid increase in the number of companies willing to report to law enforcement. It had gone all the way up to 32 percent.

You know, one victim out of three was now willing to report to law enforcement, up from 17 percent the year before, so if you have between one and two, you know, in every 100 cases you have roughly 17 reported. That is not a very high statistic.

I think there is a lot of difficulty within the corporate environment in making the determination about whether you handle this civilly, whether you cut your losses, remediate and get your business up and running again and seek damages through civil action or whether you go to law enforcement.

That is a tough call because when you go to law enforcement you get far more publicity than you might want. Then you have to worry about shareholders and investors and public relations.

Mr. MANZULLO. Loss of confidence.

Mr. CHARNEY. Loss of confidence. It is a hard call for a CEO whose primary responsibility is to protect the assets of the corporation and not to——

Mr. MANZULLO. Especially in light of the fact that the penalties are so minimal. That goes back to what you were saying. Do companies then opt for civil action, or do they just take it on the chin?

Mr. CHARNEY. No. I am actually now on the private side, and the cases that we have been investigating for companies is for civil suit purposes, not to go to law enforcement.

Mr. MANZULLO. Are these very difficult cases to try and prove?

Mr. CHARNEY. Like everything else, it is so dependent on the evidence. I mean, the Four Pillars case we had someone in the company who was being paid off. We flipped him. We put him in a hotel room. We had a camera. The president of the foreign company was going to see the Forest Hills tennis tournament. We had him stop off in the hotel room, and he traded documents for money.

The best part of the case, the documents actually said Confidential, and he took scissors and told our informant to cut out the word Confidential and throw it away where it would not be found.

That is a great case to try, but in most cases it is far more difficult, especially electronic cases because it is very hard to trace back to the source, and even if you can trace back to the source machine, it does not tell you who is the person sitting at the keyboard. If that machine is in another country, now you have to figure out if that country has similar laws.

Mr. MANZULLO. We just had that. Was it Indonesia where the——

Mr. SWARTWOOD. Philippines.

Mr. MANZULLO. In the Philippines. That shows obviously a lack of legal coverage, but only a Philippine law could apply there.

Mr. CHARNEY. That is correct. In fact, there are groups. There are three international organizations looking at some of these issues. One is the G8, and I used to chair the G8 subgroup of high tech crime, one is the United Nations, and the other is the Council of Europe.

There is a push internationally to harmonize criminal laws in the new economy area, but it is slow. It takes a lot of work. Many countries do not quite see the threat. Indeed, we have only been waking up to it.

Mr. MANZULLO. Where do you draw the line? When I asked the Assistant Director, at what point does something become espionage? You earnestly recruit people that are with other companies. That goes on all the time. At what point do you cross the line? At what point is a crime committed?

Mr. CHARNEY. I mean, generally we would look at the statutory elements first and foremost, and then I hate to say this, but it is a little like paraphrasing Potter Stewart on obscenity, which is I know it when I see it.

Most of the cases that were brought to our attention were egregious cases where, for example, people, companies, will not come to

law enforcement and report we had an employee. He got hired away by another company. We want you to go investigate.

In fact, the government would probably say that is a perfect civil suit, not a criminal one, because you are in a situation where there is going to be a lot of dispute over the facts, a lot of questions about whether it is an employment dispute or——

Mr. MANZULLO. Scott, let me followup on that. If you have an individual that works for one company and is hired away by a competitor, how much of his mind has to stop?

Mr. CHARNEY. Well, the answer is it does not. I mean, general knowledge does not have to stop, but specific does. In fact, I have seen cases where individuals who have created proprietary information then go to another company and recreate proprietary information.

I can tell you in those cases companies are looking at civil suits over that issue. They think that crosses the line because the second company is producing now the same unique product that the first company had and gave them a competitive edge in the market.

Mr. MCGUIGAN. Generally you have a non-disclosure agreement in the first place with any high level employee creating that type of information so if he breaches the contract in the first instance.

Mr. MANZULLO. A non-competitive agreement.

Mr. MCGUIGAN. Second, if he were claiming it was simply in his head, in many cases now there is what is known as inevitable disclosure. He is inevitably using the proprietary data that he got in the first instance to develop the data for another company, so those cases are prosecuted civilly.

I have been involved in them. I had someone who developed software for machinery and then when to work for another company 5 years later and developed the same software. We successfully sued them and prevented them from doing that.

Even though he claimed he did not take any of the information with him when he left, he had the process by which the flow charts for the computer software, which allowed him to essentially create it.

Mr. MANZULLO. I have one last question if you do not mind, regarding the four suggestions that you made. Mr. McGuigan, you mentioned the fact that there is no subject matter jurisdiction, that you have to have diversity in order to get the Act involved.

Mr. MCGUIGAN. Correct. You do not have a Federal Economic Espionage Act, so you sue in the states. If you were suing a citizen of another state and you get diversity, you can——

Mr. MANZULLO. Do you mean if there is no Federal Act?

Mr. MCGUIGAN. There is no Federal Act now. There is only a Federal criminal Act.

What I am suggesting is they should make the Economic Espionage Act and create a civil cause of action under the Economic Espionage Act and allow the companies to spend the resources to prosecute the cases because they will do it, and they will do it when they are confident that they can do it, and they will no longer be afraid they are going to lose control of the case and the government is going to——

Mr. MANZULLO. So do you think that is one of the problems is that there is no Federal cause of action?

Mr. MCGUIGAN. I think it is clear to me. I never thought as a state prosecutor I would be arguing for an expansion of Federal jurisdiction, but it is clear to me in this particular case.

Mr. MANZULLO. You have come to your senses. OK.

Mr. MCGUIGAN. It is clear to me.

Mr. MANZULLO. We are moving with electronic commerce that moves like that across state lines. That is a little bit different.

Mr. MCGUIGAN. I have come to the conclusion that creating a Federal cause of action is really the way to go, and I think almost everything was pointed out here today.

Mr. MANZULLO. Which could be tried in a state court. You could actually try that case in a state court if the law——

Mr. MCGUIGAN. You should not have preemption. You should have it you can file a Federal cause of action or a state cause of action. In other words, you should be allowed to file either.

I do not think there should be a preemption of state uniform trade secrets law as has happened in some other areas, so I am not suggesting that, and I am not talking about it in expansive approaches in the RICO Act. I am just talking about creating a cause of action.

Ms. ROS-LEHTINEN. Those are good recommendations.

Mr. MANZULLO. Yes. I appreciate that very much. Thank you.

Ms. ROS-LEHTINEN. I think we will move on that. Thank you so much for your excellent testimony. We appreciate it, and we will be checking back with you. I am sure as we move on this, on these recommendations. Thank you.

The Subcommittee is now adjourned.

[Whereupon, at 3:27 p.m. the Subcommittee was adjourned.]

A P P E N D I X

SEPTEMBER 13, 2000

COMMITTEES:
INTERNATIONAL RELATIONS
GOVERNMENT REFORM
CHAIR:
SUBCOMMITTEE ON
INTERNATIONAL ECONOMIC
POLICY AND TRADE
VICE CHAIR:
SUBCOMMITTEE ON
WESTERN HEMISPHERE

Congress of the United States
House of Representatives
ILEANA ROS-LEHTINEN
18TH DISTRICT, FLORIDA

PLEASE RESPOND TO:
2160 RAYBURN BUILDING
WASHINGTON, DC 20515
(202) 225-3931
FAX (202) 225-5620

DISTRICT OFFICE:
9210 SUNSET DRIVE
SUITE 100
MIAMI, FL 33173
(305) 275-1800
FAX (305) 275-1801

Ileana Ros-Lehtinen
September 11, 2000
Subcommittee on International Economic Policy and Trade
"Corporate and Industrial Espionage and Their Effects on American Competitiveness"

The past decade has brought profound changes, yet, some of the characteristics of the "old world order" continue to live on today, with some of the darker impulses of yester years adapting to fit a new time and a new set of standards and requirements.

The front line is no longer the one which divides East and West, but one defined by technological innovations. The battle lines lie in research and development. Resources designed and previously used exclusively for military intelligence gathering, are now being expanded to gather intelligence on mergers, investments, and other financial transactions. The generals are being replaced with CEOs, and the bottom line is not ideological but financial.

The threat of economic and industrial espionage looms over the horizon of the business world like a grey cloud threatening a placid sea.

Those who develop a competitive advantage over their rivals stand to make millions from their innovation. That profit is enough for some to seek an unearned advantage of their own, by indulging in corporate espionage as a quick fix solution to their creative deficiencies and their inability to remain competitive in their field.

In a survey of Fortune 500 companies, the American Society for Industrial Security estimated that, in 1999, U.S. corporations sustained losses of more than $45 billion from the theft of trade secrets. Companies reported that each had suffered 2.5 incidents of unauthorized appropriation of proprietary information. The average estimated loss per incident was calculated to be over $500,000, with most incidents occurring in the high technology and service sectors.

In another study, Pacific Northwest National Laboratory, under contract by the FBI, developed an Economic Loss Model, in an attempt to assess economic losses resulting from intellectual property theft.

PRINTED ON RECYCLED PAPER

This model determined that the misappropriation of intellectual property resulted in over $600 million in lost sales and the direct loss of 2,600 full-time jobs per year.

The same technology which has propelled our economy to unparalleled heights, is also a mechanism which allows for those practicing corporate espionage to more easily sneak into a corporation's files, gather sensitive information, and escape without a trace.

However, industrial espionage is a crime which continues to be best accomplished through low tech means and is not necessarily dependent upon high tech gadgetry. A vast majority of corporate espionage crimes do not occur in Cyberspace, but rather in person, face-to-face.

For example, key employees within a given corporation might be sought out by a rival company for information, or recruited by spies posing as consultants or headhunters at trade shows.

Competitors often examine a company's own Internet home page, where key technical employees are often listed, and craft strategies on how to lure that employee away from the firm.

This is done because information can be meaningless without the help of trained employees who understand how a particular technology is used.

A critical step was taken in 1996, with the passage of the Economic Espionage Act of 1996. Since its enactment, the United States government has prosecuted 18 cases of corporate or industrial espionage. Yet, these crimes, and the threat they pose to U.S. economic security, continue to escalate.

Some would argue that this is because we are the leading target of these crimes due to our position in the global marketplace and our technological leadership.

The U.S. produces the majority of the world's intellectual property capital, including patented inventions, copyrighted material, and proprietary economic information. Factor in the incredible ingenuity and inventiveness of the American worker, and one can easily see why this problem is so pronounced in the American workplace.

Other observers contend that, if the punitive portions of the Economic Espionage Act were strengthened to make it more costly for corporations and governments to engage in industrial espionage against the U.S., the desired deterrent effect would be achieved. Many have raised export restrictions as a strong option for the U.S. to take and have underscored the need to secure binding commitments from U.S. allies in the Organization for Economic Cooperation and Development and other international forums.

We hope to examine these and other pertinent issues during the course of today's hearing and look forward to the recommendations of our panelists on steps the Congress can take to help curtail the proliferation of economic espionage.

The Impact of Corporate and Industrial Espionage on American Competitiveness

Statement Delivered by
Sheila W. Horan
Deputy Assistant Director
National Security Division
Federal Bureau of Investigation

Before the Committee on International Relations
Subcommittee on Economic Policy and Trade
September 13, 2000

Good afternoon, Madam Chairperson and members of the committee. I am pleased to have this opportunity to appear before you to discuss the economic espionage threat, and to provide insight into the FBI's efforts to fight this serious assault on our nation's economic security.

The development and production of intellectual property is an integral part of virtually every aspect of United States trade, commerce and business. Intellectual property serves to sustain the competitiveness of the American economy, and is responsible for our nation's place as the world's economic superpower. In today's environment, intellectual property and economic information in general have become the most valuable and sought after commodity by all nations throughout the world,

and the United States, as the world's economic superpower, has become the number one target of those seeking to steal intellectual property.

Why has American economic prowess become such a tempting target? The reasons are many, though three stand out. First, the collapse of the Soviet Union has caused many foreign intelligence services to reassess their collection priorities, and redirect resources which were previously concentrated on Cold War issues. Second, military and ideological allies during the Cold War have become aggressive economic competitors. And finally, the rapid globalization of the world economy has brought about an environment in which national security and power are no longer measured exclusively by the number of tanks or warships a country possesses, but instead are measured in terms of a nation's economic and industrial capabilities. President Clinton said it well in his "National Security Strategy" report when he stressed that the strength of our diplomacy as well as our ability to maintain an unrivaled military depend, at least in part, on our economic strength.

The targets of economic espionage are varied. Advanced technologies and defense-related industries remain primary targets of foreign economic espionage activities. In many instances, these industries are of strategic importance to the United States for several reasons: some of them produce classified products for the U.S. government; others produce dual-use technology applicable to both the public and private sectors; while others develop cutting-edge technologies which

are critical to maintaining U. S. economic security. At the same time though, it is important to keep in mind that we must also not ignore attempts to acquire what may be seen as more mundane, "non-high-tech" products and services, for anything that may give a foreign nation or competitor an economic advantage is a potential target.

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 though have attempted to quantify the potential damage in dollar terms, with varying results and a wide spectrum of estimates. In the end though, all agree that the cost of economic espionage runs into the billions of dollars a year. Despite not having a single definitive dollar loss figure, there are other tangible losses caused by economic espionage. When proprietary information is stolen from American companies, Americans lose jobs, U.S. capital migrates overseas, and the incentives for research, development and new investment declines. What makes arriving at a precise dollar loss the most difficult is the reluctance on the part of U.S. industry to publicize occurrences of economic espionage. Such publicity can adversely affect stock prices, customer confidence, and ultimately competitiveness and market share. As a result, gathering the data to quantify the damage is problematic. But regardless of the exact number, all agree that the damage caused by economic espionage is significant.

Before determining how to counter the economic espionage threat, it is important to know how those bent on stealing trade

secrets carry out their activities. Our investigations have shown that the practitioners of economic espionage seldom use only one method of collection in isolation. Instead, they carry out a coordinated collection effort that combines a combination of both legal and illegal methods, thus making it all the more difficult to detect. FBI investigations have identified various methods used by those engaged in economic espionage, but the most commonly used method is the classical, time-proven technique of spotting, assessing and recruiting individuals with access to a targeted technology or information. A significant FBI investigation, which will be discussed later, uncovered just such a technique used by a foreign corporation engaged in economic espionage in the U.S.

At the same time though, while the FBI is concerned about the theft of proprietary information by foreign powers, we must also be diligent in addressing the issue of non-foreign power theft. That is, in these increasingly competitive times, theft by rival companies of one another's trade secrets is also a burgeoning and important issue. Furthermore, we are dealing more and more with employees who are stealing trade secrets from their employers and attempting to sell them to the competition, or simply using them to start their own companies.

For years, the FBI and other U.S. government agencies have developed information which clearly establishes that economic espionage is a very real and significant threat. Unfortunately though, prior to 1996, federal law was woefully inadequate in addressing the economic espionage threat. Prior to 1996, the

FBI was left to rely on federal statutes such as wire and mail fraud, which did not always address the elements of economic espionage. The FBI also relied heavily on Title 18, section 2314 of the U.S. Code - that is, Interstate Transportation of Stolen Property. This statute, which is indicative of the problem the FBI faces in addressing "new economy" crimes, was enacted long before computers or even copy machines existed. Furthermore, in recent years, U.S. courts have whittled away at the statute's meaning of "property", thus often making the law useless in addressing the theft of intellectual property. Another significant deficiency in pre-1996 law was the failure to afford explicit protection for the intellectual property in question during court proceedings. By its very nature, proprietary information derives its value from its exclusivity and confidentially. If either is compromised during the legal process, the value of the information is diminished of possibly destroyed. Rather than risk such a compromise, many companies opted to forgo what legal remedies were available. It was clear that only by adoption of a national scheme to protect U.S. proprietary information could we hope to maintain our industrial and economic edge, and thus safeguard our national security.

The urgent need for federal law addressing these deficiencies was met when Congress passed the Economic Espionage Act of 1996, which was signed into law on October 11, 1996. The Act created two new felonies. The first, found at Title 18 of the U.S. Code, Section 1831, punishes any person or company that misappropriates trade secrets while intending or knowing that their actions would benefit a foreign power of entity. Persons

convicted under section 1831 face a maximum 15-year jail sentence and up to a $500,000 fine. For organizations, the fine can range up to $10 million.

The second part of the Act, found at section 1832, punishes the theft of trade secrets for simple economic gain. This section does not require the intent to benefit a foreign entity. A violation of this section carries a maximum 10-year jail term and up to a $500,000 fine for individuals, and up to $5 million in fines for organizations.

Under the law, a trade secret is defined as any information which is reasonably protected from public disclosure, while at the same time deriving independent economic value from not being known by the public. The Act also includes a provision protecting the victim-owner's trade secrets from being disclosed during the legal process.

In an effort to address the international aspect of economic espionage, the Act grants the federal government significant extraterritorial jurisdiction. While the Act applies to illegal conduct occurring outside the U.S., the law also includes language meant to ensure that there is a nexus between the illegal actions and the interests of the U.S. Therefore, the Act applies to conduct occurring outside the U.S. if: 1) the offender is a U.S. citizen, a permanent resident alien, or an organization organized under U.S. law; or 2) an act in furtherance of the crime is committed in the U.S. Thus, actions by foreign individuals or entities overseas may still fall within the

jurisdiction of the Act.

The FBI took advantage of the new Act almost at once. In December, 1996, within two months of its enactment, the first arrest under the new law occurred in Pittsburgh, Pennsylvania. Patrick Worthing and his brother, Daniel, were arrested by FBI agents after agreeing to sell trade secrets belonging to Pittsburgh Plate Glass Company for $1,000 to an undercover FBI agent posing as a representative of Owens-Corning, a Pittsburgh Plate Glass competitor. Patrick Worthing, the first person convicted under the Act, was sentenced to 15 months in jail and three years probation.

As mentioned earlier, one of the classic methods of obtaining information, whether trade secrets or national security secrets, is the recruitment of the "insider" with access. Just such a technique was used in the following case:

Victor Lee was a long-time, trusted employee of the Avery Dennison Corporation, a U.S.-based adhesive company, when he was invited to speak before the Industrial Technology Research Institute in Taiwan. While in Taiwan, Lee was approached by a successful Taiwanese businessman, P.Y. Yang, who offered Lee a deal which he could not refuse. Yang proposed that Lee serve as a consult to Yang's company, Four Pillars, which while much smaller than Avery Dennison, was still a competitor. At first Lee declined, but was eventually convinced by a rather generous "consultant's fee", including expenses to travel to and from Taiwan. From 1989 to 1997, Lee provided Four Pillars with

Avery Dennison manufacturing and research trade secrets valued in the tens of millions of dollars. During this time, Four Pillars paid Lee approximately $160,000. Then, in late 1997, the FBI's Cleveland Division was notified by Avery Dennison that the company had discovered a corporate spy on its payroll. Avery Dennison requested the assistance of the FBI, and proceeded to provide its full cooperation to the U.S. government during the ensuing investigation and trial.

Victor Lee was eventually confronted by the FBI, and agreed to cooperate. In September, 1997, while cooperating with the FBI, Lee met in a Cleveland hotel with P.Y. Yang and Yang's daughter, Sally Yang, who served as the head of Four Pillars' research and development department. Immediately after the meeting, P.Y. Yang and Sally Yang were arrested and charged with theft of trade secrets and conspiracy. In January, 2000, P.Y. Yang was sentenced to six months home confinement, 18 months probation, and fined $250,000. Sally Yang was sentenced to one year probation and fined $5,000. The Four Pillars company was fined $5 million, the maximum fine allowed under section 1832.

Next, I would like to discuss an important case which, if it had gone against the government, would certainly have dealt a significant blow to the FBI's efforts in seeking the assistance of the corporate community in combating economic espionage.

This case involves the major cancer-fighting drug, Taxol, which is manufactured by the Bristol-Meyers Squibb Company. Taxol,

once collected from the now-endangered Yew tree, is synthetically manufactured by means of a process developed by Bristol-Meyers. This process was considered a trade secret by Bristol-Meyers.

In June, 1995, Jessica Chou, the business development manager of a Taiwanese company, began corresponding with a technology information broker by the name of John Mano. Unbeknownst to Chou, Mano was an undercover FBI agent. For more than a year, Chou and a technical director at her company, Kai-Lo Hsu, communicated with Mano to discuss how they could acquire Bristol-Meyers' Taxol trade secrets-illegally if need be.

In June, 1997, Mano met with Kai-Lo Hsu and one of Hsu's colleagues in a Philadelphia hotel. During this meeting, Hsu and his colleague were allowed to review documents relating to Bristol-Meyers' Taxol trade secrets. At the end of the meeting, Hsu and his colleague were arrested. Hsu, Chou and their colleague were charged with numerous violations, including the attempted theft of trade secrets.

As the trial date neared, Hsu and his colleague, through their attorneys, requested during the discovery process that they be allowed to review the documents which were shown to them in the Philadelphia hotel. That is, the defendants were asking to see the very documents which they had been charged with attempting to steal. But the government, citing the provision of the Act calling for the protection of trade secrets at trial,

objected to the defendants' request. Nevertheless, the trial judge in the case granted the defendants' request to review the trade secrets. Fortunately, the Act also contains a provision allowing the government to immediately appeal just such a decision before the trial may go any further. The government quickly appealed the trial court's decision, and fortunately for the government, and for trade secret owners, the appellate court overturned the trial court and ordered that the court not permit the defendants to see the Bristol-Meyers trade secrets. Without such a decision, the effectiveness of the law would have been vitiated.

After the appellate court decision, Kai-Lo Hsu pleaded guilty to the charges of attempted theft of trade secrets and conspiracy. He was sentenced to time served and two years probation. He was also fined $10,000. Jessica Chou remained in Taiwan, and was never tried. Charges against Hsu's colleague who joined him in the hotel meeting were dropped.

While these cases are an example of what the FBI can accomplish using the Economic Espionage Act, the law alone is not enough to fight this threat. The government *must* enjoy the trust and confidence of the corporate community - who are the direct victims in these cases. To this end, the FBI continues to strengthen its Awareness of National Security Issues and Response program - otherwise known as ANSIR. The ANSIR program is aimed not only at informing the private sector about economic espionage - most are already keenly aware of the problem - but also to educate them about the Act, and what the

FBI can do, with their assistance, to fight this threat. Each of the FBI's field offices has an ANSIR coordinator whose job it is to liaise directly with the private sector on this issue.

More and more, business is becoming a battlefield and intellectual property is the reward. U.S. national security and economic security are forever linked. As a result, we cannot afford to be lax in our efforts to battle this serious threat. The prevention and prosecution of economic espionage is, and will continue to be, a top priority of the FBI, for only then can law enforcement do its part in preserving a strong, innovative, and robust American economy.

Thank you for your invitation and interest in this important issue.

Statement of Dan Swartwood,
Primary Author of 1999 ASIS/PwC Intellectual Property Loss Survey and
Corporate Information Security Manager
Compaq Computer Corporation

Before the Subcommittee on International Economic Policy and Trade
Committee on International Relations
United States House of Representatives

September 13, 2000

Madame Chairwoman and members of the committee, I want to thank you for the opportunity to discuss a topic that unfortunately seems to only be addressed as a subplot in movies and an occasional sensational headline. That topic is Economic Espionage and its impact on American competitiveness. I would like to comment today on its history; its origins in the United States; discuss the impact of economic espionage on our current economy; make some forward looking projections; and then discuss what I believe is a potential course of action for the government and the business community. I am here before you due to my expertise as the author of several independent studies and the opinions I express in this statement are my own personally.

I would like to start by briefly discussing the experience underlying the opinions I will express. For 27 years, my professional career has involved all aspects of security, but specialized in information protection. As an Army counterintelligence officer, I supported both tactical and strategic goals of various military organizations from divisions to commands and joint operations. I was also given the opportunity to work with the defense contractor community on the development of highly secret weapons and communications systems. I also had occasion to work with other government agencies on a variety of issues including both continuity of government and risk to our nuclear arsenal.

Since leaving government service, I have consulted on information protection issues for the Defense On-Site Inspection Agency, commercial clients, and the Secret Service. During this time, I had the privilege to be part of a small team conducting an independent review of the White House security program. It was an honor to be a part of such a professionally rewarding effort. I left that assignment with the deepest admiration and respect for both the US Secret Service as an organization, and the men and women dedicated to protecting the President, his family and the nation's house.

I have spent the last five years working as the information security manager for what is now one of the largest companies in the United States, Compaq Computer Corporation. During my tenure at Compaq, it has grown into the

20th largest corporation and 75th largest in the world. I would like to think that the information safeguarding efforts of myself and other dedicated professionals have helped with that success by creating an environment in which the management, our workforce, and partners understand and support the need to safeguard proprietary information.
As I will explain later, such an environment is a critical factor to business success in the information age.

For the last eight years I have been privileged to serve on the National Standing Committee for Safeguarding Proprietary Information of the American Society for Industrial Security, International. This volunteer committee is made up of security professionals given the charter to create innovative safeguarding techniques and find ways to communicate the extent of and impact from intellectual property and proprietary information loss. As a major part of that effort we have conducted four nation-wide surveys.

These surveys were conducted to begin a process by which the issues surrounding business information loss could be documented and analyzed more formally. Prior to these surveys there was no systematic effort to categorize the extent of the problems associated with information loss. In the last few years other organizations and educational institutions have begun efforts to understand the scope and magnitude of the impact of information losses. We welcome these efforts to build and improve on our original surveys and expand the body of knowledge on this critical topic.

I have been fortunate to be a key contributor in all of these surveys. It has been a wonderful journey by which I have been able to influence the design and scope of these efforts. It goes without saying, however, that the entire committee has been key to the improvements each survey has seen. Indeed, the committee met this week to discuss the improvements for the next effort that will be conducted next year as part of the continuing effort. I will discuss some findings of these surveys later in this statement. As an attachment, I have included copies of the 1999 survey for the record.

Economic espionage has a long history. I believe the earliest recorded incident involves the Roman Emperor Justinian in the fifth century AD. China had been the exclusive source for silk to the world until Persian monks returning from China visited Justinian. They disclosed to him that the two key elements required for making silk were mulberry trees and silk worms. Mulberry trees were available, but silk worms were not. The monks went back to China and smuggled silk worms out in hollow canes and presented them to Justinian. The result was a new highly successful silk industry in the Roman Empire and a huge loss of revenue to the Chinese.

Many feel the originator of the industrial revolution in America was Samuel Slater. Until 1789, England carefully guarded the industrial design secrets of the textile mills that had created a virtual monopoly for the English. To protect this monopoly, England refused to allow anyone that had worked in these factories to immigrate to the United States. Slater apprenticed in one such mill, memorized the layout and plans for such a factory. With the assistance of American financiers, he was able to leave England and established the first American textile mill in Pawtucket, Rhode Island in 1789.

The beginning of the modern information revolution is often traced to the myriad of companies that were started by employees leaving Fairchild Semiconductor in California. This concentration of high technology firms began the phenomena now called the Silicon Valley. It is legend that most of these companies began using the intellectual property of their former employers. That all started to change in the early 1980's when major market leaders began to assert their intellectual property rights to protect their market share.

Intellectual property assets are more vital to the success of businesses as we enter the 21st Century. The main function of any modern organization is to create and process information. Ideas are transformed through a series of designs, communications and decisions into innovative products and services that drive our economy. Their worth is magnified by a corporation's ability to complete this transformation faster and better than their competition. Their worth is diminished when they are misappropriated or leaked.

These ideas, while often not formally "valued" by many companies are worth untold fortunes. In today's highly competitive environment it is now essential for American businesses to recognize that their intellectual assets are highly sought after commodities and are the engine driving their success.

The problem of trade secret and intellectual property theft is critical in part because 70% or more of the market value of a typical US company resides in intellectual property (IP) assets. Such assets are typically not formally valued and thus are not tracked in corporate accounting systems. In most cases the only attempts to value intellectual property involve licensing, or royalty payments. In the event of a known information loss, most corporations' first efforts involve civil law suits when the cause of the loss can be determined. There are a handful of accepted guidelines to value intellectual property, but all of them are implemented retroactively after a loss.

Since the value of IP assets is not well established, safeguarding efforts are often given lower priority when scarce resources are allocated. The safeguarding of financial or physical assets often gains priority because the value of these assets is clearly established and the loss or damage to them is readily apparent. Providing safe and secure surroundings for workers is conducive to a productive environment that helps limit legal liabilities in the event of violence issues and minimizes physical loss opportunities. This drives the majority of protection resources into physical/electronic barriers and security officer operations. These measures are absolutely essential and one hopes they have the additional benefit of a psychological affect in protecting intellectual property. In any modern corporation, intellectual property is one click away from being lost to the originator.

When most people think of information protection they equate it to the efforts to protect the computer system. Although essential, it is only part of the answer. The vast majority of information system security resources are targeted on keeping unauthorized individuals out of the system. Information systems security does so by the establishment of hardware integration, application measures and policy/procedures to safeguard the

input, transmission, storage and access to electronic versions of information. In the event of failure, the next major category of expense is intrusion detection. Intrusion detection consists of measures to detect, track and mitigate the efforts of external, unauthorized users. Successful intrusions seem to be the darling of the media.

But why do external intrusion prevention measures gain the majority of the available resources? It may well be that external intrusions gain the most media coverage. Negative publicity surrounding the external intrusions can be damaging to a corporation's or agency's public image and stock price. Senior managers can also suffer personal embarrassment when these events occur. The existence of internal problems is more easily controlled.

Information safeguarding expands significantly on information systems security. Information safeguarding must address all the environments in which corporate secrets exist. For every critical piece of data in a system, there is a one or more equivalent source of the same data. That source might be in a hard copy document or is more likely residing in the memory of one or more key individuals. Information safeguarding attempts to addresses each of these data sources.
Information systems security works on the premise that an authorized user on a system will act in a responsible manner. Information safeguarding takes a different view. In my personal experience, including discussions with peers and the results of every survey conducted, authorized users cause the vast majority of information loss, manipulation and destruction. Often the causes are inadvertent acts: a lack of training or failure to implement procedures. Intentional acts, of course, are a different story.

Intentional acts of misappropriation can be extremely damaging and challenging to detect. Most of these acts go unnoticed but cause great harm to companies. After a competitor comes out with a similar product or service, there is rarely a concerted effort to discover if the source of these outside competing products originated internally. The effort required is too great and the ability to track access and usage is often scattered or intermittent.

Managers are usually reluctant to accuse former workers of malfeasance. There are several possible explanations for this phenomenon. Many managers just cannot bring themselves to consider the possibility that an employee could or would do such a thing. The manager may fear that it will some how reflect badly on the manager. There are also considerations of how the allegations will affect the rest of the workforce. Another real consideration is just the pace of modern business. By the time evidence of malfeasance appears, is the effort required to prove such acts better used to move forward or spent in a potentially vain attempt to gain retribution?

The real value of information safeguarding lies in a multi-faceted, proactive approach to the problem of preventing information loss. It typically requires close cooperation among the corporate legal department, information technology, ethics, human resources and business units since it addresses many forms of "non-physical" harm to the enterprise, including theft, misappropriation or infringement of intellectual property rights. It must address all environments in which intellectual properties exist, namely physical, electronic and in the minds of the workforce. It is a major

victory when you can convince people that information is important not just to the accomplishment of the current project, but also to their personal success.

The loss of intellectual assets through unethical or illegal means costs businesses significant amounts and reduces new opportunities for future business success. In some extreme cases it may even result in bankruptcy. All of the evidence in the surveys, and in the experience of the Standing Committee on Safeguarding Proprietary Information members suggests that the monetary losses and other negative business impacts from theft, misappropriation and infringement will increase in the foreseeable future, unless companies take a more proactive response to these issues. Following is a discussion of the methodology used and the results of the latest survey.

The survey was sent to all Fortune 1000 companies. We received 97 qualified responses. We categorized the respondents into four groups, High Technology, Manufacturing, Services, and Financial/Insurance. The annual revenue of 40% of the respondents was less than $5 billion; 33% between $6-15 billion and 27% reported revenue over $15 billion. The statisticians at Price Waterhouse Coopers supported the results as statistically valid with a variation of plus or minus 10% for the subject population. The survey population, although including all major companies in America, is not necessarily representative of the entire US economy.

The current impacts from intellectual property losses on American corporations are clearly disturbing. Almost half of the companies responding to the latest survey indicated they have had at least one significant incident in the last 18 months. In fact over the last eight years there has been a steady climb in the number of reported incidents. The responding companies reported almost 1,000 incidents of loss. Reporting companies in the high technology group reported an average of 67 incidents each. That equates to over three incidents a month. Manufacturing companies reported fewer incidents, but the dollar impact amounted to almost two thirds of all reported direct revenue losses.

The cumulative direct dollar losses for 1997 and half of 1998, just in the Fortune 1000, were estimated to be as high as $45 billion. This figure may well not reflect the true extent of the financial losses. If a company has a gross margin of 25%, it would need to sell four dollars of goods and services just to break even for every dollar lost in intellectual property value. Many companies would need to sell five or more dollars to break even. These figures do not begin to address the opportunity losses.

The 1999 survey indicated that manufacturing companies, as a consequence of loss of research and development information and manufacturing process data, experienced the largest losses. Manufacturing organizations reported losses of nearly $900 million in 39 incidents where the value was estimated.

The most frequently reported losses were customer lists and data of high technology companies. Survey respondents noted over 226 incidents of loss of such data. Small companies (under $5 billion) suffered losses of research and development information, which could potentially harm their survival and future success. High tech companies had their largest losses

from unannounced product specifications. These losses would allow competitors to rush to market equivalent products, confuse the marketplace or limit the market for these new products.

There are two major non-revenue consequences of loss of information to most companies (especially high tech and services). The primary concern is embarrassment while the second is legal costs. It is difficult to place a monetary assessment on an intangible such as embarrassment, but the potential consequence such as loss of shareholder confidence could translate into very tangible financial losses if people abandon a publicly traded company based upon an information loss incident.

Legal expenses are very real and represent the costs to litigate or prosecute for known or suspected cases of theft or infringement, as well as any supplemental efforts to protect existing patents, copyrights and trademarks against infringements. Given that legal costs to litigate a single patent or trade secret suit may exceed $1million dollars, it is obviously very expensive to use litigation as a means of recovery.

Considering the apparent number of intellectual property loss incidents it might seem that law enforcement could play a more active role. However, the survey results indicated a reluctance to engage law enforcement. It may be that local, state and federal agencies are perceived as being ill equipped to handle the magnitude of the problem as indicated in this survey. The complexity and immediate nature of these issues require different skills than the more violent and less technologically challenging crimes that plague society.

Information loss incidents, by their nature, tend to be very difficult to investigate. Without the complete cooperation of the injured party; a well-trained staff (for both the law enforcement agency and the business), and the ability to quickly respond, these investigations are virtually impossible to conduct. There is still reluctance on the part of many companies to bring these cases to law enforcement when civil remedies are available. The loss of control is a real issue to many corporations.

There are also indications that corporate management has yet to prioritize safeguarding of information. The majority of reporting firms stated that safeguarding was only somewhat of a priority in their companies. A robust program requires resources, coordination among all business functions; developing and implementing a suite of preventative measures; having a reaction capability; and strong and continuous support from the organization's senior management. When there are a host of competing issues on a constant basis, selling the need for a comprehensive information protection effort is difficult unless there are immediate indications of such incidents and the negative impact is readily apparent.

Even when these conditions are met, companies tend to refocus priorities after the initial flurry of activity following significant losses. Most difficult of all, to permit an ongoing effort, the program must have universal buy-in. It has to be seen as a "value-add" to the business. Ultimately, selling these programs internally remains difficult because it is a given that even the best efforts can be defeated by a willing and knowing insider.

Business leaders are risk takers. Understanding and managing risk is what drives business success. Peter Bernstein in his seminal work on risk, Against the Gods, states, "When our world was created, nobody remembered to include certainty. We are never certain; we are always ignorant to some degree. Much of the information we have is either incorrect or incomplete." Business leaders need to include in their risk analysis the potential or consequences of information loss. I consider it a success when given the opportunity to provide input at the beginning of a major project. Even if my recommendations are not followed, they were considered, weighed against other issues and a conscious decision was made.

When asked if the safeguarding measures in place were enforced, the survey respondents indicated a problem. Guidelines are good, but not fully implemented throughout the corporations. Consistency, especially in international locations can be difficult. The only solution known to address this issue is to have some type of periodic audit and inspection program. As part of that program, there must be some mechanism for addressing the lack of conformance. If there is no down side risk to such non-conformance, it will continue unabated.

The secret to success with any proprietary information safeguarding program is effective marketing. Once the employees, managers and executives of the organization understand that the program is in their best interest, they are much more likely to voluntarily embrace and implement necessary measures. In my own experience, business managers are most responsive to these arguments and supportive of improvements after a major incident.

The respondents in the 1999 survey appear to believe that information systems security is not effective in their companies. Information systems security consists of policy, procedures, hardware, software, audits, and monitoring. One essential element not yet mentioned is administrative sanctions for not following the program. If there is no down side risk to ignoring such procedures then the entire program suffers and vulnerabilities increase. This is another area where a robust audit program is essential.

In large companies, the network is virtually changing constantly. Mistakes or omissions on the part of administrators can create large vulnerabilities that could be exploited both internally and externally. Many spectacular network intrusions are caused by the failure of administrators to implement known safeguards. The failure of individual users to implement proper controls also increases the vulnerability of information. The threat from individual failures may be smaller, but are the potential is so wide spread and difficult to detect, it must be acknowledged.

There is another aspect of information system security that can raise issues. In some cases, too many controls and procedures are mandated. This situation can have the unintended effect of causing business delays. Too many controls can also lead to wholesale disregard for essential protection measures. Balancing the need to keep pace with business operations and threats is always a challenge.

There is a great deal of anecdotal evidence concerning the threat from foreign governments and businesses. The survey respondents clearly indicate they believe these threats to be of minimal impact to their companies. This

was the second highest score of the entire survey indicating clear agreement. It is possible that the scope of the international involvement is not yet fully evident. These answers tend to support the proposition that information loss remains principally an insider threat. The good news is that insiders are the population over which the corporation has the best opportunity to exert influence and control. How effectively companies influence the insider populations' (employees, contractors, vendors, suppliers, partners, OEM's) views on information security are key to reducing information loss.

Just because the threat to business information is not primarily foreign does not make the problem less real or destructive. When the rightful owner is denied the full benefit of the trade secret or proprietary information, their business suffers and our economy is impacted. Every survey we have conducted has indicated the same trends: more incidents reported, bigger dollar impacts, and little improvement in senior manager priority.

I do not want to be perceived as a Cassandra. As you may remember, Cassandra was the Trojan seeress who uttered true prophecies but lacked the power of persuasion. So no one ever believed her words. The issues are too important to be addressed in merely academic terms.

My experience with the surveys, my career, and my dealings with security professionals throughout the United States lead me to the conclusion that without a fundamental perception change, the problem will only continue to grow. The challenge involves getting visibility at the board of director level throughout corporate America.

The federal government has worked diligently over the four years to engage the major infrastructure companies in a partnership to upgrade the critical information systems protection infrastructure for the utilities, finance, telecommunications, and transportation industries. This effort is greatly needed and will have a positive impact on these critical industries. Interestingly, the projected losses from scenarios and recent incidents of distributed denial of service attacks pale in comparison to the dollar losses from proprietary information losses to American industry annually. I think it is also interesting to note that the issues addressed in the critical infrastructure protection program emphasize external threats.

I believe the time is right for the establishment of a similar partnership involving business, academia, government and non-profit organizations to discuss intellectual property loss and its impact on our economy and ultimately our national security. This group could add more scientific rigor to the study of the issue; address the issue of information valuation; and offer a more focused view of the problem than the periodic snapshots we have been able to provide. The establishment of an on-going process by which companies could report issues anonymously would be essential. Such a database would drive measures that would greatly improve our understanding of the threat; impact and successful methods to better prevent loss of critical business information.

I want to thank you for the opportunity to address the subcommittee today and would be pleased to answer any questions you might have.

PREPARED STATEMENT OF SCOTT CHARNEY BEFORE THE SUBCOMMITTEE ON INTERNATIONAL ECONOMIC POLICY AND TRADE, COMMITTEE ON INTERNATIONAL RELATIONS, U.S. HOUSE OF REPRESENTATIVES

SEPTEMBER 13, 2000

Mr. Chairman and Members of the Subcommittee: thank you for inviting me to testify about the impact of corporate and industrial espionage on American competitiveness.

As you know, I am now a Principal at PricewaterhouseCoopers (PwC), and I work within the Investigations practice. Prior to joining PwC, I was Chief of the Computer Crime and Intellectual Property Section at the United States Department of Justice. As a result of my employment, I have had the opportunity to investigate economic espionage cases in both the public and private sector. Suffice to say, everyone now recognizes that the protection of intellectual property is critical to economic survival and success in the digital age. At the same time, the fact that such information is created, stored and transmitted in digital form makes it ever more susceptible to theft, and we must therefore be cognizant of the pervasive risks and threats that face our businesses, our government and our nation as a whole.

One sensible place to start is with the scope of the problem, and to recognize that economic espionage is only one part of a larger problem: companies suffer losses from an array of intellectual property offenses including copyright violations and counterfeiting. In a global economy, both the crime itself and the economic impact on the victim company may reach worldwide proportions. For example, in one case worked on by my firm, a company that manufactures computer parts learned through returns to its customer service department that someone was counterfeiting their hardware, including the packaging, manuals and driver software. In the course of the investigation, the firm found invoices and purchase orders for the counterfeit goods as well as hard-copies of e-mail correspondence between the suspect parties. By making purchases through a dummy company, we were able to identify United States distributors of bad parts in Singapore, Korea, Denmark and Hong Kong.

Today, it is estimated that more than 70 percent of the market value of a typical United States company resides in its intellectual property (IP) assets.[1] That this property is at risk is clear: a 1999 survey conducted by PricewaterhouseCoopers and the American Society for Industrial Security found that nearly $45 billion of information was lost in a 17-month period.[2] Particularly at risk are manufacturing processes and research and development information. The number of reported incidents of theft of proprietary information increased dramatically between 1998 and 1999.[3]

In addition to the ASIS study, the Computer Security Institute (CSI) has conducted surveys of computer security issues and trends since 1996. In the most recent (2000) survey, 90% of respondents (mostly large corporations and government agencies) detected computer security breaches within the last twelve months. Of the 585 respondents, 20% reported the theft of trade secret information. As for dollar losses, the survey found that, as in previous years, "the most serious financial losses occurred through theft of proprietary information (66 respondents reported $66,708,000)...."[4]

To some extent, these surveys may reveal only the tip of the iceberg; virtually all computer crime experts agree that most computer crimes are neither detected nor reported. This supposition was confirmed by the United States Department of Defense which, in a controlled

---

[1] "Trends in Proprietary Information Loss Survey Report," American Society for Industrial Security, International and PricewaterhouseCoopers LLP, 1999, p. 4.
[2] Id. at 28.
[3] Id. at 3.
[4] www.gocsi.com/prelea_000321.htm.

study, attacked 38,000 of its own machines. The attacked machines were successfully penetrated 65% of the time. System administrators at the successfully attacked sites detected only 4% of these penetrations. Of that 4%, only 27% reported it. Put another way, of the 38,000 machines attacked, 24,700 were penetrated, only 988 realized it, and only 267 reported the attack. This in an agency with better security than most civilian agencies and private companies.

That corporations may be in the dark about the scope of the threat is also revealed in the CSI study, which found that 32% of respondents did not even know if they had been a victim of computer abuse. In part, this reflects the nature of electronic theft. If I steal a car, the victim knows because his car is gone. But if I steal design plans for a new product, the "original" remains with the owner and, absent deprivation, the victim may go forward blissfully unaware that the crown jewels have been lost. Additionally, in PwC's experience, companies sometimes fail to identify intellectual assets within their possession. Because of that failure, they neither value nor track the asset,[5] and may not protect it adequately.

It is worth noting that the threat to companies takes different forms, many of which have little to do with the new economy. Dumpster diving for corporate information, which was a key component of the Legion of Doom hacker case involving Bell South over a decade ago, has recently returned to the news. Additionally, the first case tried under the Economic Espionage Act of 1996 was a somewhat traditional case, with a foreign company paying an insider at a United States company to pass critical paper documents.

But technology and economic trends will pose greater challenges for several reasons.

First, the Internet features of global connectivity, lack of authentication, and lack of traceability make it a wonderful medium for committing crime.

Second, the amount of data that can be stolen increases dramatically in an electronic environment.

Third, as companies encourage remote computing, data is stored on easily stolen devices (such as laptops) or on home computers not readily subject to the protective measures put in place by a company. For example, some companies have well-configured access controls and firewalls to protect data when stored in corporate computers, but nonetheless allow employees to download sensitive data to their home computers where such protections are lacking.

Fourth, as more companies form joint ventures and rely upon outsourcing, they take outsiders and move them inside electronic perimeters, even though these individuals may not be carefully supervised by, nor owe any allegiance to, the initial contracting company.

Fifth, the employer-employee relationship is changing. Unlike the older cradle-to-crave model where an employee might have spent his or her entire career with a single company, today's workplace is far more unstable. Companies are volatile and offer less stability, and workers often seek new opportunities and new rewards instead of remaining with an existing employer. In this environment, there is some increased risk that mobile employees may take trade secrets with them as they change employment. Indeed, since joining PwC, I have worked on several cases involving employees who have e-mailed apparently sensitive files to personal accounts, or even directly to competitors, shortly before changing employment.

---

[5] Ibid., p 4

Economic globalization will also pose challenges. For example, United States trade policy has long focused on opening up foreign telecommunications markets to United States carriers, certainly a laudable goal from an economic perspective. As a matter of reciprocity, however, we must also be prepared to accept that foreign companies may wish to own parts of the United States telecommunications infrastructure, a point driven home by several recent announcements by foreign companies expressing an interest in our telecom and Internet assets. In the past, phone phreakers -- i.e., hackers who specialize in attacking telecommunications switches -- have displayed the ability to wiretap phone calls. To the extent our economic competitors own United States telecommunications assets, there is the risk that proprietary information traversing those lines can be surreptitiously intercepted, with such crimes being extremely difficult to detect.

As the world continues to change, it is of course important that both companies and Congress act swiftly when necessary. For companies, it is critical to clearly identify assets worthy of protection; assess the threats to these assets (including insiders, hackers, and competitors); develop and implement physical, technical and legal protective measures (such as access controls to physical space, network security measures, and confidentiality agreements); educate employees on the need to protect trade secrets; and, finally, test the efficacy of internal policies and controls.

As for the Congress, on October 11, 1996, both the National Infrastructure Protection Act and the Economic Espionage Act became law, the latter providing the first comprehensive federal protection for trade secrets. That law does require, however, at least one minor change. Specifically, the law provides protections for trade secrets that are related to or included in "a product that is produced for or placed in interstate or foreign commerce." See, e.g., 18 U.S.C. § 1832. A trade secret can be stolen, however, even before it is placed in produced product or interstate commerce. This loophole should be closed.

In closing, I would like to thank the Committee members for their attention, and offer to answer any questions.

Statement Of
Austin J. McGuigan, Managing Principal
Rome McGuigan Sabanosh, P.C.
Before The
House Committee on International Relations
Subcommittee on International Economic Policy and Trade
September 13, 2000

Madame Chairperson and Members of the Subcommittee:

Thank you for inviting me to address your concerns regarding the effects of corporate and industrial espionage on America's global competitiveness. I am prepared to address the issues of corporate and industrial espionage and measures available for the protection of American intellectual property.
As you know, to a great degree, "the business of America is business", and in the new millennium, the strength of America's business will be in its intellectual property. Indeed, America's economic renaissance can be traced directly to its technological prowess. Maintaining the confidentiality of trade secrets is thus no longer just for the benefit of the trade secret owner, but has become one element in maintaining America's strong economic position. While theft of intellectual assets is nothing new (as reflected in a survey conducted by the American Society for Industrial Security and PricewaterhouseCoopers, and released in April,
1999) there has been a dramatic increase in the theft of proprietary information in recent years. The globalization of the marketplace, while providing American business with new opportunities, has likewise exposed American businesses to threats from foreign competitors.
Corporate and industrial espionage is certainly a two way street. Competitive intelligence, the techniques employed by businesses to lawfully and ethically obtain information about competitor businesses, is certainly a useful tool. By way of example: Car manufacturer A may purchase a car from car manufacturer B, take it apart, and "reverse engineer" some or all of its components and, to the extent not protected by a patent, incorporate them into its new car. This is a legitimate competitive undertaking. The information obtained will enable manufacturer A to improve its product, attract customers, make more sales and increase income. The resultant competition invigorates the economy to the benefit of consumers and businesses alike.
Large corporations have staff devoted to this practice and/or may instruct sales and marketing staff to pursue information through business contacts, observations in the field, business journals and other sources of public information. Businesses may also hire investigators to develop and manage one-time or ongoing company-specific competitive intelligence plans. The small proprietor performs many of these functions him or herself. A competitive intelligence program will likely have well-defined objectives, methods, reporting, analyses, monitoring and company oversight. This is to be expected and encouraged.
Business counterintelligence, on the other hand, involves related conduct, and is employed by businesses to protect against disclosures of intellectual property assets to competitors. A solid program of counterintelligence will include a well-developed understanding of what needs to be protected, for

how long, from whom and what the business' vulnerabilities may be. Businesses attempt to learn what competitors are interested in, how competitors are seeking to obtain information, and then try to short-circuit the outward flow of business information.

This may seem like a game, and indeed, it may feel like a game to some. However, it is no game when businesses that succeed or fail lose millions of dollars due to theft of their intellectual property. Put into context, as reported by Mr. Swartwood, who will also be speaking today, Fortune 1000 companies have incurred intellectual property losses of more than $45 billion during 1999 alone.

The states have, for years, provided remedies, both civil and criminal, for the protection of intellectual property. In October, 1996, the federal government weighed in with the enactment of the Economic Espionage Act ("EEA"), which proscribes an attempt to steal, a conspiracy to steal or an actual theft of trade secrets, as well as the receipt, possession or purchase of the same.

Under the EEA, a wide range of conduct may be treated as criminal. The statute protects trade secrets including "all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if . . . (A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public." 18 U.S.C. § 1839.

Punishment under the EEA may be imposed on individuals and on businesses that engage in unlawful corporate espionage. Individuals acting within the context of a local violation, one not intended to benefit a foreign government, may be sentenced to ten years in prison and/or fined $250,000 for a violation; organizations can be fined as much as $5 million for such an offense. 18 U.S.C. § 1832. Espionage on behalf of a foreign government may exact greater punishment including imprisonment of up to fifteen years and/or fines of up to $500,000 for individuals and fines of up to $10 million for organizations. Courts are further empowered to impose injunctive relief and compel criminal forfeiture under either circumstance. 18 U.S.C. §§ 1834 and 1836(a).

But how effective has the EEA been in deterring trade secret theft? That is difficult to say, as there have only been twenty or so cases prosecuted in the last four years. Given the explosion in intellectual property theft, its inevitable impact on private sector business losses and the potential compromise of national economic security, this is a surprising statistic. So why isn't the EEA being more widely utilized as a prosecutorial tool? The dearth of cases may or may not be attributable to the lack of budget allocated to EEA prosecutions, or may be the result of business entities that are concerned about placing their intellectual property, their life blood, in the hands of the government.

First, the Act is not a tool available at the discretion of a business. It provides no civil remedy. Rather, the determination of whether a reported violation will be prosecuted or not is left to the Attorney General, or her designee. Therefore, the act of reporting a suspected crime does not necessarily result in prosecution. The Attorney General, in turn,

considers, inter alia, the scope of the activity involved, evidence of the involvement of a foreign government or instrumentality, the degree of injury to the trade secret owner, the type of trade secret misappropriated, the effectiveness of any available civil remedy, and what deterrent value may come of the prosecution. Viewing the EEA as a weapon against foreign espionage, it could be deemed a failure, given that, of the twenty cases pursued, only two involve allegations against foreign business entities or their owners. See, for example, U.S. v. Hsu, 155 F.3d 189 (3d Cir. 1998) and U.S. v. Yang, 74 F. Supp.2d 724 (N.D. Ohio 1999).

Second, although prosecutors to date have been successful at obtaining guilty pleas, the statute, as written, embodies several substantial defenses that must be overcome relating to proof of intent. See Joseph F. Savage, Jr., Carol E. Didget, The Economic Espionage Act: A Promise Unfulfilled?, Intellectual Property Law Weekly (November 12, 1999).

Third, even if the government is willing to take up the cause, businesses may not want to rely on the government to prosecute the matter since the government's duty runs not to the business entity per se, but to society at large. Thus, conflicts of interest may arise between the government and the business entity with respect to whether and how the case is pursued. Likewise, depending on the facts of each situation, a business may not want the burden of cooperating with governmental investigations and/or sting operations.

Fourth, where a complaint alleges the actual theft of trade secrets, there are circumstances under which the court may compel disclosure of the very information that the business has sought to keep secret. This can occur when evidence is considered material, such as when a defendant has asserted a defense of impossibility or another defense that raises the issue of whether the information at issue should be treated as a trade secret or not within the meaning of the EEA. See U.S. v. Hsu, supra, 155 F.3d at 205-06.

Lastly, but significantly, a business that reports trade secret theft to the government must anticipate that the trade secret loss will become public information. Disclosure of such a loss may thereafter effect public and investor confidence in the business, its management and its products and cause the business further harm. See United States v. Hsu, 185 F.R.D. 192 (E. D. Pa. 1999)

Where do we go from here? It appears at this point that Congress should seriously consider creating a private cause of action under the EEA. Certainly, all states provide a private right of action, under common law, the Uniform Trade Secret Act or other legislative enactment. State court civil prosecutions can lack the desired deterrent effect, however, especially in the area of taking discovery, enforcement of injunctions, and executing on judgments. Privatizing a prosecution under the EEA would place the power of the federal courts directly into the hands of businesses, which may proceed to enjoin ongoing misappropriation and unlawful use of their intellectual property. The EEA could be amended to provide a vehicle for pre-suit discovery, with private-sector subpoena power, enabling affected parties to identify and target the appropriate offender without alerting it to an impending lawsuit. This would be most effective where a foreign entity might abscond with technology and/or hard assets to a haven beyond the territorial jurisdiction of the United States courts.

Experience shows that parallel private and governmental prosecution of intellectual property theft will benefit the business entity involved as well as the public's interest in maintaining national security and fostering continued economic growth. Amending the EEA to provide a private cause of

action will also assist in the creation of a comprehensive body of federal law in the area of trade secret misappropriation.

For the purpose of efficiency and accuracy, it would be advisable to impanel experts in this field to draft the legislation needed to control, rather than react to, unlawful behavior associated with intellectual property.

In addition, whatever law is in place to serve the salient purpose of protecting against intellectual property loss should be accompanied by programs designed to educate those who are most likely to effect the loss, such as, employees, former employees and workers of both domestic and foreign businesses in the fields of software, computers, engineering, and other technical, scientific and manufacturing sectors, with an emphasis on those with ties to nations known to be engaged in illegal corporate espionage.

Rather than just having employees sign non-disclosure agreements, specific plans should be implemented to inform them of when conduct that might otherwise be acceptable as competitive intelligence crosses the line to illegality. This is important not only to educate the unlearned and prevent loss, but also because knowledge is an element of many intellectual property crimes. Proper education would thus ensure knowledge of a minimal degree, eliminating ignorance as a defense in those instances. Naturally, businesses have an incentive to inform their employees. However, there may be programs the government can sponsor that would assist with this objective, especially in the area of foreign entities engaging in such illegal activities.

That concludes my remarks. If you have any questions, I would be glad to address them.

ECONOMIC ESPIONAGE ACT
CASE SUMMARIES

[As of April 13, 2000]

TAB	CASE NO.	CASE NAME	DISTRICT	STATUS
1	97-CR-323 97-1965	United States v. Kai-Lo Hsu, Chester S. Ho, and Jessica Chou	Eastern District of Pennsylvania	(HSU) Indicted 7/10/97, Trial 4/5/99. Pled guilty. Sentenced 7/13/99 (Time served plus probation, $10,000 fine.) Chester S. Ho was dismissed.
2	97 CR 288	United States v. P.Y. Yang, et al.	Department of Justice Computer Crime and Intellectual Property Section	Indicted 10/1/97, Trial 3/22/99 Found guilty 4/99 on two EEA counts Sentenced 01/05/00 (Four Pillars: $5,000,000 fine; P.Y. Yang: $250,000 fine, 6 months home confinement, 2 years probation; Sally Yang: $5,000 fine, 1 year probation)
3	97-00124	United States v. Steven L. Davis	District of Massachusetts	Pled guilty Sentenced 4/17/98 (27 mos. impr.; 3 years supervised release; $1,271,171.00 restitution)
4	H-97-251S	United States v. Mayra Justine Trujillo-Cohen	Southern District of Texas	Indicted 11/14/97 Pled guilty 7/30/98 to one count of economic espionage Sentenced 10/26/98 (48 mos. impr.; 3 yrs. supervised release; $337,000.00 restitution; $200.00 special assessment)
5	98-CR-059	United States v. Carroll Lee Campbell, Jr. ("Athena") Northern District of Georgia	Northern District of Georgia	Indicted 2/25/98 Pled guilty 5/27/98 Sentenced 8/25/98 (3 mos. impr.; home confinement 4 mos. with electronic monitoring detention; 3 yrs supervised release; $2800 restitution; $100 special assessment.)

6	97-9	United States v. Patrick and Daniel Worthing	Western District of Pennsylvania	Indicted 2/25/98 Pled guilty 5/27/98 Sentenced 8/25/98 (3 mos. impr.; home confinement 4 mos. with electronic monitoring detention. 3 yrs supervised release; $2800 restitution; $100 special assessment.)
7	98-059	United States v. John Fulton	Western District of Pennsylvania	Pled guilty 3/98 Sentenced 11/13/98 (12 mos. home detention, 5 yrs. probation)
8	98-80943 98-00300	United States v. David T. Krumrei	District of Hawaii	Indicted 5/14/98 Pled guilty 7/27/99. Sentenced 11/18/99. (Two years imprisonment, $10,000 restitution, $100 special assessment)
9	4:98M37	United States v. Steven Hallsted and Brian Pringle	Eastern District of Texas	Pled guilty Sentenced 12/4/98 (HALLSTED) (77 mos. imprisonment; $10,000 restitution) (PRINGLE) (60 mos. imprisonment; $50,000 restitution)
10	98-48-P-H	United States v. Caryn L. Camp and Stephen R. Martin	District of Maine	Indicted 9/16/98 (CAMP) Pled guilty to 15 counts 7/22/99 Sentenced 12/7/99 (3 years probation, $7,500 restitution. $1,500 special assessment). (MARTIN) Trial 8/9/99. On 8/16/99, jury returned a guilty verdict on 8 of 15 counts, including mail fraud, wire fraud, conspiracy to steal trade secrets and conspiracy to transport stolen property. Sentenced 12/20/99 (366 days imprisonment, 3 years supervised release, $7,500 restitution. $800 special assessment.)
11		United States v. Huang Dao Pei	District of New Jersey	Pending

12	98-200-70-0 1-EEO	United States v. David Sindelar	District of Kansas	Information filed 10/16/98 Pled guilty to theft of trade secrets Sentenced 3/1/99 (5 yrs. prob.; $16,618.35 restitution; $10,000 fine; $100 special assessment)
13	99 CR 15 DFL	United States v. David B. Kern	Eastern District of California	Indictment filed 3/5/99
14	H-99-158 Judge David Hittner	United States v. Robin Carl Tampoe	Southern District of Texas	Indictment filed 3/24/99 Pled guilty 8/2/99 to counts #2 (attempted theft of trade secrets) and #3 (forfeiture) of superseding indictment. Count 1 (theft of trade secrets) of the superseding indictment, and both counts of the original indictment, were dismissed at sentencing. Sentenced 10/25/99 (15 months imprisonment, followed by 2 years' supervised release. Judge Hittner made a finding of no ability to pay a fine and did not impose a fine. Ordered to forfeit $5,000 in cash, special assessment of $100.)
15		United States. v. Eon Joong Kim (3COM)	Northern District of Illinois	Complaint filed July 1999 Complaint dismissed without prejudice October 1, 1999
16	99-CR-174	United States v. Matthew R. Lange	Eastern District of Wisconsin	Indictment filed 9/7/99 Convicted 12/10/99 of violating the EEA, Copyright infringement, and wire fraud. Sentenced 03/02/00 (30 months imprisonment, 3 years supervised release, $2,500 fine, $525 special assessment.)
17	CR H-99-623	United States v. Oliver P. Costello	Southern District of Texas	Charges filed 10/28/99 - - one count of theft of trade secrets Pled guilty 02/25/00 Sentencing scheduled for 06/05/00
18		United States v. Tejas Procurement Services	Northern District of Texas	All defendants pled guilty 12/9/99 to conspiracy to steal trade secrets.
19		United States v. Mark Everheart	Western District of Pennsylvania	Pled guilty 03/30/00. Sentenced 03/30/00. (1 year probation, $100 special assessment.)

20		United States v. Say Lye Ow	Northern District of California	Indicted 03/29/00.

Go to . . . CCIPS Home Page || Justice Department Home Page

Last updated May 15, 2000
usdoj-crm/mis/mdf