S. HRG. 105—489

CYBERCRIME, TRANSNATIONAL CRIME AND INTELLECTUAL PROPERTY THEFT

HEARING

before the

JOINT ECONOMIC COMMITTEE CONGRESS OF THE UNITED STATES

ONE HUNDRED FIFTH CONGRESS

SECOND SESSION

March 24, 1998

Printed for the use of the Joint Economic Committee

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1998

cc 48-750

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-057323-8

JOINT ECONOMIC COMMITTEE

[Created pursuant to Sec. 5(a) of Public Law 304, 79th Congress]

Prepared for printing by DARRYL C. EVANS,
COLLEEN J. HEALY AND
JUANITA Y. MORGAN

CONTENTS

OPENING STATEMENT OF MEMBERS

WITNESSES

SUBMISSIONS FOR THE RECORD

CYBERCRIME, TRANSNATIONAL CRIME AND INTELLECTUAL PROPERTY THEFT

Tuesday, March 24, 1998

UNITED STATES CONGRESS,
JOINT ECONOMIC COMMITTEE,
WASHINGTON, D.C.

The Committee met at 10:15 a.m., in Room SD-680 of the Dirksen Senate Office Building, the Honorable Jim Saxton, Chairman of the Committee, presiding.

Present: Representatives Saxton and Ewing; Senator Robb.

Staff Present: Christopher Frenze, Mary Hewitt Juanita Morgan, Colleen Healy, Andrew Quinlan, Joseph Cwiklinski, Dan Lara, and Darryl Evans.

OPENING STATEMENT OF REPRESENTATIVE JIM SAXTON, CHAIRMAN

Representative Saxton. The Joint Economic Committee (JEC) hearing will come to order.

Good morning. The hearing this morning is on cybercrime, transnational crime, and intellectual property theft and, in particular, the role the Federal Bureau of Investigation (FBI) plays in this arena.

Cyberbanking is now a growing part of our everyday lives. The information is easy for us to use, but it's also vulnerable to tampering and theft.

The proliferation of technology has increased the opportunities for conducting economic espionage. The theft of trade secrets has cost billions of dollars in losses.

Foreign governments actively target U.S. companies and the United States Government as well in order to steal our capital technologies and information.

To begin to better understand these emerging economic and national security threats, as a first step, we have three very knowledgeable gentlemen from the FBI with us this morning:

Deputy Assistant Director Neil Gallagher of the Criminal Division.

Deputy Assistant Director Larry Torrence of the National Security Division; and

Assistant Director and Chief Michael Vatis, National Infrastructure Protection Center.

I would obviously welcome you all this morning. And I understand that there has been a case study entitled, "Intellectual Property Theft – Economic Analysis Case Study," which I would like to ask unanimous consent at this point be made a part of the record.

Thank you, gentlemen for being with us this morning. We appreciate very much the effort that you have made to be here and for the time that you're willing to give us this morning.

Obviously, have busy schedules and we very much appreciate you being here.

Deputy Assistant Director Torrence and Deputy Director Vatis and Deputy Assistant Director Gallagher, we appreciate your participation.

Deputy Assistant Director Gallagher, if you would like to begin, please.

[The prepared statement of Representative Saxton, along with the "Intellectual Property Theft – Economic Analysis Case Study" appear in the Submissions for the Record.]

STATEMENT OF NEIL J. GALLAGHER, DEPUTY ASSISTANT DIRECTOR, CRIMINAL DIVISION, FEDERAL BUREAU OF INVESTIGATION

Mr. Gallagher. Thank you, Mr. Chairman.

I have submitted an official statement for the record and I'll just make a few brief comments.

I welcome this opportunity to provide insight into the FBI's efforts in the fight against economic crime to include transnational crime.

Economic crimes affect a wide variety of industries, businesses, and citizens. The theft of trade secrets has caused billions of dollars in losses and created a vulnerability within all types of industry.

The significant and most positive advances in technology have also allowed businesses and financial institutions to become prey of a new age of criminals. The World-Wide Web has allowed for an endless barrage of frauds, scams, intrusions and piracy.

Cyberbanking has added a new dimension of potential financial institution fraud.

The FBI's task in fighting economic crime has dramatically changed with advancements in technology. New methods of economic crimes are being addressed with the assistance of new laws passed by Congress such as the Economic Espionage Act of 1996 and the No Electronic Theft Act.

At the same time, there is an increased emphasis on the training of FBI agents and providing them with the tools necessary to investigate these often complicated investigations.

The number of thefts of trade secret investigations has continued to increase. The increase is due in part by the positive relationship that the FBI is developing with private industry and the resulting increased awareness of this crime problem.

At the same time, we must recognize that technological advances are making corporate spying and theft easier and cheaper. The power of computer technology has increased the means for the theft and transfer of trade secret information. Computer age communications connectivity, commercial enterprise activities, and the posting and accessibility of corporate data on office work stations and home personal computers have made it extremely easy to copy and steal valuable trade secret information.

And yet, another area that you mentioned already, cyberbanking, is redefining consumer banking and creating new opportunities for high-tech financial institution fraud.

A recent Internet survey indicated that electronic banking is anticipated to increase 600 percent in the new two years.

In the latter part of 1997, the Federal Deposit Insurance Corporation estimated that over 1100 banks and thrifts are maintaining a presence on the World-Wide Web. Although many sites are primarily established for advertising, a growing number are beginning to offer transactional capabilities, including fund transfers.

Cyberbanking was the victim in 1994 when subjects in Russia gained unauthorized access to Citibank's cash management system. As a result, more than $10 million was wire-transferred to pre-established accounts throughout the world.

Fortunately, in the end, all but $400,000, taken before the FBI entered the investigation, was recovered.

The investigation resulted in six foreign nationals being charged with this crime. The ringleader, Vladimir Levin, was arrested by Scotland

Yard and was extradited to the United States from England in September 1997. He plead guilty on January 23rd, 1998, to conspiracy.

In response to the cyberbanking threat, the FBI, in cooperation with the Department of Justice and Department of Treasury and representatives of financial regulatory agencies, has launched a cyberbanking initiative to examine the risks and potential losses associated with electronic banking.

A working group has been established to focus on current and potential criminal activity in this emerging field.

The primary function of this working group is to ensure that all government agencies involved with the operation or regulation of cyberbanking are aware of the potential for fraud.

A secondary function is to ensure that adequate fraud prevention measures are implemented so that frauds against the system can be detected, investigated and prosecuted.

The banking industry has not been the only industry dramatically affected by Internet fraud. The copyright industry has lost millions of dollars due to piracy of software, music, and interactive digital software on the Internet.

Downloading music free of charge from the Internet is becoming increasingly popular. The music industry stands to lose substantial sums of money because of the unauthorized distribution of its copyrights.

Bulletin board services have long been a potential source of computer, software and interactive digital software piracy. There exist bulletin board services whose only function is to engage in criminal activity. These bulletin board services provide a listing of software programs available for downloading through the Internet. The actual cost of the software involved is negated through a bartering system.

Software piracy, as well as all other types of piracy, continues to be an international concern. According to the International Intellectual Property Alliance, copyright piracy cost an estimated loss of $10.8 billion annually to U.S. copyright industries. In addition, the International Anti-Counterfeiting Coalition has estimated the annual cost due to trademark infringement in the world to be $250 to $350 billion annually.

To conclude, a major concern now facing law enforcement is how rapidly the threats from criminals, both domestic and international, are changing, particularly in terms of technology.

The challenge to law enforcement is our ability to keep pace with these criminals who pose a threat to the United States, our citizens, and our industries.

The FBI is working closely with law enforcement officials in other countries to combat computer crimes and enhance coordination, and improve our combined capabilities.

Cooperative efforts with industry have also been intensified to facilitate the prevention and detection of emerging cyber crimes.

The types of economic crimes described today can and do have a lasting effect on our nation's economy. The FBI is aggressively investigating these types of economic crimes.

Mr. Chairman, I wish to thank you for your support. I applaud your commitment and interest in this important area of the FBI's responsibility.

Thank you.

[The prepared statement of Mr. Gallagher appears in the Submissions for the Record.]

Representative Saxton. Mr. Gallagher, thank you very much.

With your permission, I'd like to hear from the other members of the panel, and then I have some questions.

Would that be all right with you?

Mr. Gallagher. Certainly.

Representative Saxton. Thank you very much.

Mr. Torrence, please proceed with your testimony. Incidentally, we're going to proceed in a more relaxed atmosphere than normal. We have those two little lights in front of you there which are supposed to indicate when five minutes has elapsed.

However, because of the situation this morning, we'll be able to take a little bit more time than that. So feel free to proceed at your pace.

STATEMENT OF LARRY E. TORRENCE, DEPUTY ASSISTANT DIRECTOR, NATIONAL SECURITY DIVISION, FEDERAL BUREAU OF INVESTIGATION

Mr. Torrence. Thank you, Mr. Chairman. And thank you for this opportunity to join my colleagues in providing the FBI's perspective in this area of growing concern.

As Mr. Gallagher has indicated, economic crimes have a serious impact on a wide variety of industries and businesses, and therefore, upon the economic well-being of the United States.

The ever-increasing value of proprietary economic information and the global and domestic marketplaces, and the new uses for technology, have combined to enhance the opportunities and motives for conducting economic espionage.

Foreign governments and major foreign industrial sectors play a prominent role in their nation's business intelligence collection efforts. While a Cold War military rival stole military secrets about a state-of-the-art weapon or defense system, today's economic rival steals proprietary business information or government trade strategies.

As a result, the intelligence agencies of some governments conduct economic espionage against the United States. These governments actively target U.S. persons, firms, industries and the government itself, to steal our critical technologies, patented formulae, and business plans on behalf of their own economies.

Because trade secrets are an integral part of virtually every aspect of U.S. trade, commerce, and business, the security of trade secrets is essential to maintaining the health and competitiveness of critical segments of the U.S. economy.

In 1994, the FBI established its economic counter-intelligence program as part of our national security strategy. The passage of the Economic Espionage Act of 1996 has greatly assisted us in our battle against those who conduct economic espionage. The Act resolves many gaps in federal criminal laws.

It fundamentally modernized our criminal code by protecting intellectual property through strong new criminal sanctions.

Principally, the act created two new felony crimes. The first of the two, Title 18, U.S. Code, Section 1831, punishes any person or company that steals trade secrets on behalf of a foreign government or entity. Persons convicted under this law face a maximum 15-year sentence and up to a $500,000 fine. For organizations, the fine can range up to $10 million.

The second crime, which is Section 1832, punishes the theft of trade secrets for simple criminal gain and does not require the intent to benefit a foreign entity. It carries a maximum 10-year jail term and up to a $500,000 fine for individuals and a $5-million fine for organizations.

Under the law, a trade secret is defined broadly as any proprietary information that is reasonably protected from public disclosure and that derives independent economic value from being a secret for the rightful possessor.

Importantly, the act has a provision protecting the victim's trade secret from public disclosure throughout the entire court process.

Prior to the passage of this act, the FBI was already addressing hundreds of foreign counter-intelligence investigative matters concerning hostile economic intelligence activities.

That pace continues. The FBI has developed significant information on that foreign economic threat to include identification of foreign government sponsors of economic espionage, the economic targets of their intelligence and criminal activities, and the methods used to clandestinely and illicitly steal U.S. Government information, trade secrets and technology.

Additionally, the FBI has forged crucial partnerships with the Department of Defense, Department of Energy, other government agencies, and private industry, to allow for prompt detection and successful investigative efforts in this area.

A number of countries continue to pursue economic collection programs. Foreign economic collection focuses on science and technology, as well as research and development. Of particular interest to foreign collectors are dual-use technologies and proprietary economic information which provide high profitability.

Proprietary business information, such as bids, contracts, customer and strategy information, is aggressively targeted. Foreign collectors have also shown interest in government and corporate financial and trade data.

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

An intelligence collector's best source continues to be a mole or trusted person inside a company or organization whom the collector can task to provide proprietary or classified information.

Recently, we have seen the international use of the Internet to contact and task insiders with access to corporate proprietary information.

Other methodologies include the recruitment of foreign students, joint ventures, and the use of well-connected consultants to operate on behalf of a foreign government.

In conclusion, the FBI must continue to address the ever-present threat to intellectual property, trade secrets and other proprietary economic information. The evolution of the global community and of technology itself presents a rapidly changing arena in which the foreign threat to U.S. trade secrets is constantly lurking.

The FBI's efforts to build key relationships with other executive departments and with private industry will be crucial in the successful counter-intelligence efforts focusing on the economic collection activities of foreign entities.

Thank you for your time and your support of this critical area of concern to the national security of the United States.

[The prepared statement of Mr. Torrence appears in the Submissions for the Record.]

Representative Saxton. Mr. Torrence, thank you very much. We appreciate your very fine and thoughtful testimony.

Before we proceed to Mr. Vatis, let me just welcome Mr. Tom Ewing, a Member of Congress from the State of Illinois.

Today is an incoming travel day, I guess we call it around here. Members are traveling back to Washington at this hour. We hope that we'll be joined by several other Members as we proceed as they arrive here in Washington.

Mr. Vatis, you may proceed. Mr. Vatis is Assistant Director with the National Infrastructure Protection Center.

Sir, thank you very much for being with us. You may proceed.

STATEMENT OF MICHAEL A. VATIS, DEPUTY ASSISTANT DIRECTOR AND CHIEF, NATIONAL INFRASTRUCTURE PROTECTION CENTER, FEDERAL BUREAU OF INVESTIGATION

Mr. Vatis. Thank you, Mr. Chairman, Congressman Ewing.

With your permission, I'd like to enter my formal statement into the record and deliver a few minutes of abbreviated remarks this morning.

Representative Saxton. Without objection. Thank you.

Mr. Vatis. As we continue to rush into the Information Age, our society is moving increasingly on-line. We use computers, the Internet, and other new information technologies to conduct business, perform scientific research, engage in personal communications, and conduct a whole host of other activities.

But as we as a society are moving on-line, so are criminals. And as my colleagues have discussed, criminals use the Internet to defraud unsuspecting senior citizens, disseminate child pornography, steal credit card numbers, and rob banks by electronically shifting funds to their own off-shore accounts.

But the Internet and other advances in information technology do not merely give criminals new means to commit traditional crimes like theft or fraud. They also allow criminals and other malicious actors to cause new types of harm that go well beyond the potential loss to the individual victim and that can affect our national economy and, indeed, our national security.

What type of harm am I talking about?

The everyday functioning of our economy depends on the delivery of certain critical services. While we once got along fine without electrical power, think of the consequences if the power went out for a week across the whole Eastern seaboard.

There are several services like electrical power whose availability we may take for granted, but which are truly critical to the smooth functioning of our society.

We call these vital services our critical infrastructures.

Executive Order 13010, signed by President Clinton in 1996, lists the following eight infrastructures as critical to our economic health and national security: telecommunications, banking and finance, transportation, electrical energy, gas and oil, water, emergency services, and government operations.

These infrastructures are critical because their debilitation or destruction would have a significant adverse impact on our economy or national security.

Here in the United States, we're able to expect things to work because our infrastructures are highly developed and efficient. We can wake up in the morning confident that the lights will work, that water will flow from the tap, and that the trains will run. And businesses can plan

their activities and investments around the certainty that they will have ready access to telecommunications, that gas or oil will supply power to their factories, and that their goods will be transported.

It is a given in both our personal and professional lives that essential goods and services will be available when needed.

Not so long ago, our dependence on these infrastructures did not pose a significant problem because there was little risk that these vital services could be knocked out. Only a rare occurrence like a tornado or an earthquake or a power outage could knock out a critical service over a broad area.

The physical breadth of these infrastructures made it difficult for a potential bad actor to cause anything other than an isolated disturbance.

And our geographic isolation from other countries made it difficult for foreign adversaries to launch an attack on our infrastructures.

The Information Age, however, has changed things dramatically. All critical infrastructures now rely on computers and advanced telecommunications, including the Internet, for the control and management of their own systems, for their interaction and communication with other infrastructures, and for communications with their suppliers and with their customers.

Electrical power grids and natural gas pipelines, for example, are controlled by computer systems, and those computers may be linked to each other and to the company headquarters by publicly accessible telecommunications systems and commercially available information technologies to allow efficient management of power generation and smooth delivery to customers.

Billions of shares are traded each day over the telephone or over the Internet, and the stock exchanges could not function today without their vast networks of computers.

But this reliance on new technologies comes with a price, and that price is a new vulnerability to those who would cause us harm. For just as the new technologies make it easier for companies to communicate and control their businesses, they also make it easier for malicious actors to cause harm.

This new vulnerability stems in part from the inherently open nature of the Internet and modern telecommunications systems. This means that with a certain amount of technical skill, one can use these commun-

ications media to get inside a company's or a government agency's computer system without ever physically penetrating its four walls.

This vulnerability is exacerbated by several factors.

First, most of our infrastructures rely on commercially available, off-the-shelf technology. That means that a vulnerability that may exist in one company also exists in many other companies across the country.

Second, our infrastructures are increasingly interdependent and interconnected with one another. The banking system, for instance, depends on the availability of the telecommunications system and the Internet, which in turn rely on electrical power.

This interdependence makes it very difficult to predict the cascading effects that the disruption of one infrastructure would have on all the other infrastructures that it's tied to.

Third, our telecommunications infrastructure is now truly global. There's no such thing anymore as a National Information Infrastructure. There's only a Global Information Infrastructure.

This means that our geographic isolation from other countries no longer acts as a moat to fend off foreign adversaries.

As the Citibank case that Mr. Gallagher talked about demonstrates, it's now just as easy to break into an infrastructure's computer network from St. Petersburg, Russia, as from St. Petersburg, Florida.

So that's the vulnerability picture. But what about the corresponding threat?

In the physical world, the range of people or groups that would have the means and motive to cause widespread destruction of an infrastructure are relatively limited. Terrorist groups and hostile nations are the most likely actors.

But the accessibility of the information infrastructure, global connectivity, and the rapid growth of a computer-literate population combine to ensure that millions of people around the globe now possess the means to engage in a cyber attack.

The spectrum of threats in this new cyber world is staggeringly broad and it includes the disgruntled insider who seeks revenge against his employer or former employer, the recreational hacker out to test his cracking skills against attractive targets, organized crime groups seeking illicit financial gain, domestic or international terrorist groups bent on causing harm to send a political message, foreign intelligence services seeking companies' proprietary data or sensitive government information,

and hostile nation-states utilizing information warfare as part of, or instead of, a strategic military attack.

Now some people think this vulnerability and this range of threats is overstated, and that we have sufficient technological security tools in place to protect against malicious hackers and crackers, and that the infrastructures have built-in redundancies to protect their systems against a catastrophic failure.

But I'm afraid that the facts prove otherwise.

Although we haven't experienced the electronic equivalent of a Pearl Harbor or an Oklahoma City, as some people have foretold, the statistics and our cases demonstrate our dangerous vulnerabilities to cyber attacks.

To give you just two statistics, a 1998 study by the Computer Security Institute shows that 64 percent of the companies polled reported information system security breaches, an increase of 16 percent over last year. The total financial losses from the 241 organizations that could even put a dollar figure on their losses adds up to over $136 million. This represents a 36-percent increase over last year.

In 1996, the Defense Information System Agency, the agency that oversees all of the computer and telecommunications systems for the Defense Department, estimated that as many as 250,000 attacks on DoD systems occurred the year before. And DISA indicates that the number of attacks has increased significantly for the past few years and that it expects this trend to continue.

And we at the FBI have seen a significant increase in the number of our own computer intrusion investigations. Pending cases have increased 115 percent from the beginning of fiscal year 1997, from 260 to 480 pending investigations that we have right now that involve just computer intrusion cases.

In fiscal year 1997, there was a 110-percent increase in indictments and a 950-percent increase in arrests.

Let me now give you a couple of examples of the types of cases we've seen in recent years.

You're undoubtedly aware of the recent series of intrusions into Department of Defense and other government agency computers across the country. This case involved widespread illegal intrusions at the government systems using holes in the system's software.

I can't go into detail on this because it's a pending case, but the FBI recently identified two juveniles in California who appear to have been

responsible for many of the intrusions. And the Israeli National Police, working with FBI, Air Force, and NASA investigators, this week placed under house detention an individual who also appears responsible for many of these attacks.

We're still examining the extent of harm caused by the intrusions, but the potential harm was obviously enormous because even the unclassified systems used by DoD and other government agencies contain an enormous amount of important and sensitive data, the loss or alteration of which could have serious adverse consequences for our national security.

You've also probably read about the plea bargain in Massachusetts last week of a teenage hacker who was able to break into the former NYNEX system and through it, disable telecommunications at a regional airport, cut off services to the airport's control tower, and prevent incoming planes from turning on the runaway lights.

I think this case is a real wake-up call for those people who would argue that hacking is simply harmless fun, or actually provides some sort of public service by alerting us to our vulnerabilities.

Representative Saxton. May I just interrupt you for a moment on that point?

The interruption of the lights at the airport are an example of somebody getting into a system by way of a computer route?

Mr. Vatis. By way of a computer route and the public telecommunications system, yes, sir.

Representative Saxton. Okay. Thank you.

Mr. Vatis. Now let me tell you what the FBI is doing about this problem.

On February 26th of this year, the FBI created the National Infrastructure Protection Center. Our mission at the center is to detect, deter, respond to, and investigate unlawful acts involving computer intrusions and acts, both physical and cyber, that threaten our critical infrastructures.

This means we don't simply investigate and respond to attacks after they occur, but we try to learn about them and prevent them before they happen.

This requires the collection and analysis of information gathered from all available sources and the dissemination of our analyses and of

warnings of possible attacks to potential victims, whether in the government or in the private sector.

This broader mission also means that we in the FBI and law enforcement as a whole can't do this alone. This mission really requires the combined efforts of many different agencies. The Defense Department has a critical role to play because its reliance on information technologies makes it a prime target for our adversaries, and because DoD holds much of the government's expertise in the cyber realm.

Our intelligence agencies have a critical role to play because of their responsibility for gathering information abroad about foreign threats.

And civilian agencies with jurisdiction over critical infrastructure, such as the departments of treasury, energy, and transportation have similarly significant roles.

But this also isn't just a job for the Federal Government. State governments have to be involved because they own and operate some of the critical infrastructures and because their law enforcement agencies and other agencies are often the first responders in the event of a crisis.

And most importantly, this mission requires the intensive involvement of the private sector. Private industry owns and operates most of the infrastructures and also has the greatest expertise in the technical problems and solutions, so they have to be part of the effort to invent solutions and implement them.

In recognition of all the roles that these other entities play, the NIPC is founded on the notion of a partnership that includes all of the critical federal agencies, state and local law enforcement, and private industry, and our intent is to foster the sharing of information and expertise and improve coordination among all of these actors in the event of a crisis.

Let me note finally that we've only been in existence for less than a month, so we're very much in the early stages of building the Center and we have a lot of work to do as we move forward in building the necessary liaison with other agencies and with the private sector. An this will take some time.

But I think the FBI has taken an important first step in establishing the Center and in recognizing the need for an inter-agency and public/private partnership as we move towards the challenges of the 21st century.

And, Mr. Chairman, I think your holding this hearing indicates that you and Congress also recognize the significance of this problem and the

need for new solutions. And we look forward to working with Congress on this important matter.

Thank you.

[The prepared statement of Mr. Vatis appears in the Submissions for the Record.]

Representative Saxton. Mr. Vatis, thank you very much.

Let me begin the questions here this morning by a question for each of you that's intended to help members of the panel understand precisely what it is that each of you do.

In the context of cybercrime, in the context of what's referred to as transitional crime and intellectual property theft, Deputy Assistant Director Gallagher, can you explain to us in a very simple way because we need simple explanations, particularly when it comes to this subject, what it is that the criminal division does relative to transnational crime, as well as these other items that we have mentioned here several times?

Mr. Gallagher. Let me approach that question from two different perspectives.

The FBI's criminal investigative division is responsible for all criminal investigations throughout the United States. Traditionally, financial institution fraud would be one major area of our investigation.

So as you in your opening comments, Mr. Chairman, commented upon the impact of cybercrime in the United States and its impact on financial institutions, the FBI's criminal investigative division would be concerned about that area.

Perhaps a very straightforward way of looking at this is the Economic Espionage Act of 1996 resulted in two sections of the criminal code.

Section 1832, theft of trade secrets, is really focusing on an aspect of theft of trade secrets as we would look at it in a traditional sense – pure criminal activity to steal a trade secret from one company.

More often than not, it's by a disgruntled employee who is leaving a company, going to a competitor and trying to barter that company's trade secret.

Those are the areas that the criminal division is focusing on, along with other responsibilities for organized crime, the other traditional economic crimes.

And the difference as we talked about cyber-crime is all of the traditional economic crimes that we've known for many decades still exist. It's the method by which these crimes now will be enacted that has changed somewhat dramatically, resulting in a different investigative approach by the FBI.

Representative Saxton. Thank you. Mr. Torrence, the National Security Division also has, I'm sure, a different and specialized role to play here.

Would you describe that for us as well?

Mr. Torrence. Yes, Mr. Chairman. The National Security division is the part of the FBI that's responsible for national security matters, and traditionally has focused on foreign counter-intelligence and espionage investigations, and we're continuing to do that.

But the world has changed and we've seen foreign governments, including foreign intelligence services, that have a great expertise in stealing information, where in the past it was national defense information, military information, classified information, are using those resources to go after economic secrets as well.

The economic security of the United States is part of the national security of the United States. So we have to protect it just as diligently.

The American corporations and companies are no match for a foreign intelligence service that's been doing this for decades and generations.

So our investigations under economic espionage is, as Mr. Gallagher explained, both parts of the act.

The espionage part is the first part, which requires that a foreign government or an entity of a foreign government or a foreign corporation be involved in stealing United States proprietary information, stealing trade secrets.

If they are involved in that, a foreign element, then that is the economic espionage part of that act.

So the national security division focuses on that. We train on that. But we also conduct investigations that result in the straight criminal trade secret theft which is the second part of that act as well.

Representative Saxton. Thank you. Mr. Vatis, let me pose a question in a slightly different way.

What is the mission of the National Infrastructure Protection Center?

Mr. Vatis. It's a broad one, Mr. Chairman.

Representative Saxton. I gather. I could tell that you're more of a specialist in terms of the world of computers rather than in law enforcement, as we generally and traditionally think of it.

Mr. Vatis. I think in one sense we are specialized in that we are focusing on cyber-intrusions, although we are also looking at physical threats to the infrastructures.

But we are also broad in the sense that we really straddle the two FBI's divisions, the Criminal Investigative Division and the National Security division, because we utilize both sets of authorities – both criminal investigative authorities and counter-intelligence and counter-terrorism authorities.

And that stems from the unique nature of cyber-cases, which is that when you first notice an intrusion, you have no way of knowing what it is. You don't know if it's a 15-year-old hacker who's just trying to test his skills. You don't know if it's a cyber-terrorist. And you don't know if it's a foreign intelligence service trying to gain sensitive proprietary data.

And it's not until you investigate a case, almost to the end, if not to the very end, that you can actually say, okay, this was a case involving one of those possible threats.

And so you have to have at your disposal all of the different authorities that we are able to use to conduct an investigation.

It turns out, I think, that the vast majority of our cases turn out to be straight criminal investigations that involve criminal acts by people within the United States.

But we're also focusing on the threat that would cause the greatest harm, the threat of a cyber-terrorist or a foreign nation-state using cyber means to attack our critical infrastructures as a means of attacking the United States.

That's where our focus is, on deterring, detecting, and preventing those types of attacks, and assessing the information that we gather from our own law enforcement investigations, from state and local law enforcement, from the intelligence community, and from information we get voluntarily from the private sector; analyzing that information, to see if we can draw conclusions about vulnerabilities that exist, about threats

that are out there, about trends that we might be seeing; and using that information to try to prevent attacks before they happen.

But in the event that attack do occur, we will work with our field offices to investigate, and we will coordinate the government's overall response to an attack.

Representative Saxton. Well, thank you very much. You know, I can't help but reflect on my time here in Congress as it relates to this subject.

I came here a little over 13 years ago and I remember walking into my office and seeing a computer keyboard and a terminal and a mechanical printer that was enclosed in a case to try to protect our ears from the noise.

I know Mr. Ewing is younger and he doesn't remember those types of devices, but we did have them here when I came.

Anyway – he didn't think it was funny.

(Laughter)

The reason I mention that is just to demonstrate to all of us the incredible change that has taken place. I often say to my friends, I have no idea what I did without a fax machine and I have no idea what I did without a cell phone.

I can't imagine dealing with the volume of information that society deals with today without the benefit of the developments that have taken place in the area of cyber over the short period of time that I've been here.

It's quite incredible. And to think of the vulnerable aspects that have developed along with this, that we have perhaps not begun to address in the serious way that perhaps we should have, that it's good to know that there are those of you who have begun – not only begun, but are obviously effectively dealing with these issues in some very, very serious ways.

Mr. Vatis, when you were discussing your efforts, one of the points that you made which I think is extremely important is that not only do we deal with information here in the Congress of the United States, but you listed a number of areas which made me think, or to conclude, I guess, that it's virtually impossible to think of almost any aspect of American life or international life where we aren't so completely immersed with the use of computers that the lack of the ability to use those facilities and the information that we gain from them for any period of time would be quite catastrophic in the way we do business today, wouldn't it?

Mr. Vatis. I think that's right. People are aware of their reliance of computers in their everyday lives, but I don't think they're aware of things like electrical power and telecommunications, and even gas and oil delivery, that depend on computers for their every day functioning.

So if you brought down the computer systems that are responsible for delivering those supplies, it would have cascading effects on their infrastructures. I don't think anyone has been able to map out these cascading effects. What would happen, for instance, if you were able to cut off the flow of natural gas through a pipeline from Louisiana to the northeast?

What would be the effects on telecommunications or the banking industry if power were cut off at power plants in the northeast?

There are those sorts of second- and third- and fourth-level effects that I don't think anyone has yet been able to determine because our infrastructures are so interdependent on one another.

It's not just that we wouldn't be able to use our computers at our desks in our offices or in our homes, but it would be all of those other things that we rely on just to get by in everyday life that would be adversely affected.

Representative Saxton. Let me ask a question that relates to something that we dealt with about a month ago here in the Committee.

We held a hearing which focused on radio frequency mechanisms – weapons, if you will – that have the effect of interrupting computer capability.

Is this something that you deal with, Mr. Vatis? And put this in the context of a threat level as compared to other threats that we deal with.

Mr. Vatis. Radio frequency weapons are something that we would put into the category of cyber-weapons, even though we talk mostly about the use of computers and attacks over the Internet as the most common example at cyber-attacks. But radio frequency weapons can be used without having to rely on an Internet connection.

As long as an attacker is in the vicinity of computers, they can be used to cause the same sort of denial of service attack.

So, that's something that we're looking at as well.

That is not something that traditionally has been a law enforcement concern. It's been something that the military has been concerned about because our military, being the most advanced technologically in the

world, has learned about the need to protect its sophisticated information systems from radio frequency attacks and the like.

On the civilian side, we have not really focused on the harm that could be caused by those types of weapons. But that is one of the cyber-weapons that we've been looking at, along with other things.

Representative Saxton. And are radio frequency weapons and the use of them, is this an issue that is central to the job that you do, or is it a less serious threat than that?

Mr. Vatis. I'm not sure how to characterize the threat.

I think what I can say is that we have not seen many instances, if any, where somebody has used a radio frequency weapon for an attack in the civilian world.

But it is certainly a potential form of an attack, so it's on our list of concerns.

Representative Saxton. But the threat pose that you deal with by hackers and crackers, as you put it, is something that is more common place in the more traditional way of stealing information or getting information in an unauthorized fashion and of disrupting computer services?

Mr. Vatis. Much more commonplace because, in effect, all you need is a computer and a modem to connect you to a telecommunications system and the Internet. And if you have the technical wherewithal in your mind, you can use those simple tools that are found in millions of homes throughout the country to launch an attack.

And in fact, nowadays, you don't even need great technical expertise yourself to launch an attack because there are websites that you can go into and find automated tools that you can simply download on to your own system, compile the source code, and click on a button to launch the attack.

So it's a ready-made tool for someone who merely has to find the website and download the program. He doesn't have to invent his own sophisticated program to do an attack.

So it's increasingly easy to do.

Representative Saxton. Let me just ask one final, one more question, before we move to Mr. Ewing. And let me just address this to all three of you, if you don't mind.

Explain to us – we understand that the FBI has a very important and central role to play in law enforcement in this area.

But what role does the private sector have to play? Do you coordinate your efforts with the private sector in any way? And is the private sector concerned? And if so, what has the private sector done to try and enhance security?

Mr. Gallagher. A critical aspect of any success we'll have in cyber-crime relies on the coordination and cooperation that we have with private industry.

Earlier, I had mentioned the Citibank case and that's quite frequently mentioned when the FBI talks about the prospects of cybercrime.

I think one important aspect of that is the fact that Citibank, once they identified the first signs of the potential problem, reached out to the FBI and brought us into the investigation.

The fact that they did that allowed the FBI to begin to track the transferring of this money around the world, resulting in solving the case and, fortunately for Citibank, greatly minimizing the impact on that financial institution.

If the FBI is to be successful, we have to have the cooperation with private industry, and to use their expertise in this area.

The FBI, by itself in isolation, will not be able to conduct these types of investigations, Every time we come into one of these investigations, a new area of technical expertise rises up.

Not long ago, we had a computer intrusion case primarily in Northern Florida that someone was hacking into a 911 system for local police agencies.

This became very critical because, essentially, the hacker could tie up the 911 calling system, preventing a citizen from being able to simply dial into a 911 because all they would get was a busy signal.

That raised a whole new area of FBI investigative interest, trying to understand how the 911 system for the State of Florida was created, which resulted in us having to go out to private experts to develop that expertise, eventually resulting in the successful conclusion of that case.

So our relationship with private industry has become even more dramatic with the advent of cyber-crime.

Representative Saxton. Thank you. Mr. Torrence?

Mr. Torrence. Regarding economic espionage, the role of industry is critical.

First, the theft of a trade secret must be reported to us by the company that lost the trade secret. And by the very nature of that, if a company is concerned that by coming to the FBI, that the legal process will cause them to lose the very trade secret that they're attempting to protect, then they will not come to us.

So the role of industry has grown increasingly, particularly with the new economic espionage law.

That law specifically directs the court to protect the trade secret during court proceedings. We are working very closely with industry to educate them on the law and how we will conduct those investigations and the type of assistance that we will need from them.

We reach out to industry both in personal ways as well as electronic means and virtually reach tens of thousands of these companies.

I think we have reached out to about 25,000 companies or corporations and in the last year, we made about 60,000 presentations or communications to companies on this area. And the result is positive.

Companies are being cooperative. They are becoming more confident and knowledgeable of the law and how it's being investigated.

So they are very critical players in economic espionage.

Mr. Vatis. I'd like to just reiterate what my colleagues have said by saying that a fundamental mission of the National Infrastructure Protection Center is to reach out to the private sector and establish liaison relationships and actually include representatives from the private sector in our Center to try to foster the sort of cooperative relationship and information-sharing that is necessary for us to do our jobs. Because if private industry doesn't tell us about the intrusion cases that they're seeing, we won't know about them and we won't be able to gather the information that we need to conduct analysis and to disseminate warnings about vulnerabilities and threats that are out there.

And we won't be able to perform what is a fundamental law enforcement mission – to prosecute cases so as to deter future criminals from engaging in criminal activity.

I think industry is increasingly seeing the long-term picture, which is that they can't keep their sensitive intrusion cases to themselves. If they do, then there will be no one out there performing the deterrence

function because criminals will believe that they can engage in hacking or other forms of criminal activity with impunity.

Only through law enforcement can we deter criminals from engaging in such activity.

Representative Saxton. Thank you.

Mr. Ewing?

OPENING STATEMENT OF REPRESENTATIVE THOMAS W. EWING

Representative Ewing. Thank you, Mr. Chairman, and thank you for holding this hearing. It's a very interesting subject.

When you tell a joke, though, just tell me ahead of time and I'll be sure and laugh because when the Chairman jokes, every member should laugh.

What do you think – and unless I direct a question to you, any of you can give me your answer.

Is the greatest danger to property or to safety?

Mr. Gallagher. Let me jump in with a property argument, and then I'm sure I'll defer to a safety argument because I guess it would take the incident.

If there were an incident today that threatened the security and safety of the people of the United States, that would certainly take prominence.

But at the same time, when we talk about the economic welfare of the United States, if there were a significant cyber-banking institutional fraud that affected Wall Street, that would be a grave concern.

So I don't know that you can look at one versus the other.

From a pure criminal investigative perspective, we are concerned with the economic aspects of it and the livelihood of the U.S. industries that depend upon these telecommunications systems and computer systems.

But I don't know that there is a simple answer, to be straightforward with you, that I would put one over the other.

Mr. Torrence. We won't gang up on the safety issue, but regarding property, it's hard to quantify the loss of intellectual property, although we've attempted and in fact, the study that the Chairman mentioned was an effort that we made to try to put some kind of a quantification to that.

That's quite an interesting study, though laborious reading. But maybe I can summarize it to try to put a dollar value on it.

This was a study that we asked the Northwest Pacific National Laboratory to do for us, to try to come to a method in determining what intellectual property amounts to.

How do we quantify it if it's stolen?

And that's a case in which an American company which had a joint venture with a foreign firm, foreign licensees, and a product that would be sold overseas as well as in the United States, that information was stolen by a foreign competitor who captured the market.

And the conclusion of that big study is that this misappropriation of intellectual property in this particular case resulted in over $600 million in lost sales, the direct loss of 2600 full-time jobs and a resulting loss of 9542 jobs for the economy as a whole over a 14-year period, trying to project that down the line.

And it also determined that the trade balance was negatively impacted by $714 million and lost tax revenues of $129 million.

So it's difficult to put a dollar value on it, but that's the best effort that we have. And in the cases that we are seeing, we are seeing loses that we project to be in the hundreds of millions of dollars in aggregates.

The dollar figures are very large.

Mr. Vatis. If it's difficult to quantify in dollar value the loss of sensitive proprietary data, it's even more difficult to quantify safety costs, or the loss of lives.

I think only plaintiffs' lawyers can even try to put a dollar figure on the loss of life.

I think, undeniably, most of the cases that we see will involve property loss or economic loss. But the potential impact on safety is really a serious one.

I think the Massachusetts case that I talked about, in which a plea bargain was announced last week and which involved a hacker who shut down air traffic control at a regional airport, really demonstrates the possible safety consequences in the real world, in the physical world.

I think there are people out there who still romanticize hackers as kids just having fun or performing a service by demonstrating the software glitches in DoD systems or in private-sector systems without

realizing the physical world consequences that can result either advertently or inadvertently from hacking incidents.

Mr. Gallagher mentioned the 911 case. How do you quantify the impact on an elderly person who can't get through to 911 in an emergency because a hacker has tied up all the phones?

Those are real consequences.

If somebody is able to use a hacking tool to disrupt electrical energy to the northeast in the dead of winter, how do you quantify the physical impact on people who can't heat their homes or can't drive to the store or drive to the doctor?

Again, there are those second-, third-, and fourth-level impacts that are very serious, but that people don't realize can result from what seem like just activities in the cyber world, which some people think of as ethereal and unreal.

There are real-world consequences that people have to be aware of.

Mr. Gallagher. Maybe if I could just add to what's been said here, we should almost be sitting here holding hands because it doesn't make much difference if the risk is security or an economic risk.

It's the techniques that the criminals, terrorists, or intelligence agencies would use against the United States, are all identical. There is a constant sharing of information and sharing of approach.

There is one FBI investigative approach to these types of investigations that's just spread amongst the three components that you see here before you today. And that's the important aspect, to bring the FBI up to the ability that we're able to conduct these types of investigations and prevent, whether it be an economic or a security threat to the United States.

Representative Ewing. I would assume the black-outs that we had on the east coast sometime back would be an example of the kind of chaos that could come out of these activities.

All of you are with the FBI. Would you feel that the Administration, this government, the government as a

whole – I'm not thinking just about the Clinton Administration – is putting a high enough priority on the danger that is out there from possible interruptions and property?

Mr. Vatis. I'll take a crack at that. I think it is. I think this is really an instance in which the government is getting ahead of the curve rather

than waiting for some sort of electronic Pearl Harbor or Oklahoma City to occur and then taking action after the fact.

In 1996, the President formed a presidential commission on infrastructure protection to assess the nation's vulnerabilities to cyber and physical attack on our infrastructures and make recommendations.

And the Administration is in the process now of considering which of those recommendations of the commission to implement.

I think this hearing, hearings that the Congress has held in the past year or year-and-a-half, on this issue demonstrate that Congress, the Legislative Branchs also recognizes the importance of this problem and the need to take action in advance of some catastrophic disaster.

So I think we are addressing the problem appropriately. We are still in the process of figuring out concretely what we need to do long-term to assure that we have a sufficiently educated work force not only at the FBI, but also in other agencies, so that we can take the necessary preventive measures, and things like that.

How much we need to appropriate to all of the various efforts in the government to address this problem is another area that we're looking at now.

But I think the awareness level is sufficiently high.

Representative Ewing. Do we have, and will it come out of these recommendations, this commission, the type of legislation we need to put on the books to address the criminal activity here?

Do we have the right type of criminal laws on the books to give you in law enforcement the authority to aggressively pursue?

Mr. Gallagher. I think one positive answer is the Economic Espionage Act of 1996 was a dramatic step in that direction.

Prior to that, we almost had to engage in creative prosecution because we had to look at other violations associated with the crime to try to press charges against it.

With the advent of this new act and the resulting statutes, we have a more direct, solid tool that we can use to combat this type of crime.

Mr. Vatis. The other statute that I would mention is the set of amendments in 1996 to the Computer Fraud and Abuse Act, 18 U.S. Code, Section 1030. Those amendments made it much easier for us to prosecute unauthorized intrusions into not only government computer

systems, but also private-sector computer systems that affect interstate or foreign commerce.

And so, again, we don't have to utilize other statutes creatively. We have a specific statute now thanks to Congress' amendments that address unauthorized computer intrusions.

Representative Ewing. Would you see this as being an area of the law that would be confined to prosecution of federal cases?

We have a dual system in America with state laws and federal laws. And if so, if this is going to be the purview of the federal prosecution, the federal law enforcement people, do you have the capability of handling that if it's widespread, or should there also be state involvement in setting up the laws to protect us?

Mr. Torrence. I think in the area of espionage, as the law is written, I think it's best that the Federal Government retain that.

We have the remainder of Title 18 that we've used for many years. It's a very complicated topic. It's difficult for locals, I think, to get involved in that.

So I think the Economic Espionage Act is right on target, it's effective, and I think it's better to be retained in the federal system.

Mr. Vatis. I think there is a role for state and local law enforcement. But I think in the cyber world, one of the difficulties is that you don't know where an attack is coming from in the early stages of an investigation.

You also can have multiple targets that are affected by the same attack in many different states and, indeed, around the world.

So I think it's difficult for a state or local law enforcement agency to try to investigate a case where the attacker may come not only from another state, but from another country.

And there may be so many different victims in different states, that it really becomes something that the federal law enforcement community has to be actively involved in in order to deal with all of these multiple attacks in one coherent investigation, rather than having perhaps 50 state or local investigations covering the pieces within their jurisdictions.

Mr. Gallagher. But at the same time, one of the real successes of the FBI has been our coordination with state and local law enforcement.

We're certainly not going to walk away from it. They, in many respects, will be responsible for the jurisdiction or the localities where the crime or the crime victims may exist.

So they're going to have a very direct role.

In the 911 case, the local law enforcement were in fact the victims. We work very closely with local law enforcement in the State of Florida to try to better understand where potentially this threat could be coming from.

So we're going to work still closely with state and local law enforcement. But Mr. Vatis is right. The computer doesn't have any boundaries.

One of the real secrets, or the simple aspects of our investigation, we don't try to make a decision when we get the first intrusion, whether it's coming from a foreign intelligence source, a foreign terrorist, or a straight criminal.

What we're looking at is the methodology by which the attack is occurring and finding the facts out as it develops.

Representative Ewing. Well, you went right to the next question. You could see exactly where I was going, Mr. Gallagher, because I wondered about cooperation with the local law enforcement people.

And I'm glad to hear that that is in fact taking place.

Is there any kind of a planned organization to bring along the local law enforcement at the state level and from our major cities who might have the expertise to work with the FBI?

Mr. Gallagher. Let me focus in on cyber-banking and financial institution fraud because in just about every major city in the United States, the FBI will have a very active, productive relationship with local law enforcement to protect financial institutions.

To the extent that the crime becomes a cyber-banking attack on a financial institution, we will bring in and use the expertise of the FBI, use the expertise of local law enforcement. In different locations, they may have a unique expertise. They may have unique contacts with private industry that will advance the cooperative relationship and cooperative investigation.

So Mr. Ewing, you're perfectly right. We must use the capabilities of local law enforcement and we are in fact doing that.

Mr. Vatis. We're doing two things, also, very concretely.

One is we're bringing into the National Infrastructure Protection Center representatives from state and local law enforcement to try to help us establish the necessary liaisons with local law enforcement across the country

We also have a training unit that is responsible for coordinating the development of training curricula and programs, not just for our own FBI cyber investigators, but also for other agencies in the Federal Government and for state and local law enforcement. Even though we have a tremendous need to build expertise within the FBI and in all 56 field offices, I think state and locals have an even more pressing need to develop that expertise because they have not had as much experience to date in dealing with computer investigations.

But I think they are inevitably going to have many more cases to deal with.

And so, we want to try to bring them up to speed on those types of cases.

Representative Ewing. I would assume that if you're working with the locals, you're also working internationally with our friendly nations around the world to address this on an international scale, also.

Mr. Gallagher. There have been international law enforcement conferences just on the specific topic of cyber-crime.

It truly has to be an international solution to it because there are no boundaries.

One of the difficulties in conducting these types of investigations, you enter into the systems – for example, I'll go back to the 911 case.

As we developed the attack, we brought it to Atlanta, Georgia, where it was going through an AT&T conference call system. It came in in one aspect of the conference call capability and went out over to London, England. We tracked it over to London, England with the assistance of British authorities and from there, we tracked it on to another conference call capability that was being washed through this conference call out to Sweden.

And so, in one simple case, very quickly, we found ourselves investigating activity that was emanating out of Sweden all through the computer. And it involved the assistance cooperation of Sweden, Great Britain and the United States to solve this crime.

Representative Ewing. Do you think we put the story out and maybe, I guess, not being very computer-literate, I don't maybe understand the question you may think I should.

But that people who use computers and what they can do, how they can get into another person's system and they can cause this problem. Is that something that's being disseminated among our young people and in our schools about some type of what's criminal, what isn't criminal?

Mr. Vatis. I think that's a critically important area. I don't want to get out in front of the President's decisions, but I think one of the recommendations of the President's commission was to have an education program, to try to develop curricula for kindergarten through graduate schools to try to teach ethics in the computer world. Because as kids become technically proficient, they have to understand the ethical, moral and legal implications of what they're doing on-line.

It's a matter both of allowing parents to protect their children from some of the things that are not necessarily the most savory things on-line, but also a matter of teaching children what they should or should not be doing on-line because of, again, the ethical and legal implications.

Representative Ewing. Do you believe that there will be some – there probably will be, but do you think it's pretty obvious there will be a need for additional legislation at the federal level to implement the President's recommendations and stiffer penalties, stiffer criminal laws to govern this area?

Mr. Vatis. I think there may be a need for some legislation, but, again, I don't want to get out in front of the Administration's decisions on that.

Representative Ewing. Do you think we aren't quite ready and know exactly what we need to do in that regard, then?

Mr. Vatis. I think there will be some proposals probably coming out of the Administration, but what those proposals are, I don't know yet.

Representative Ewing. Finally, I was interested in your knowledge about the encryption legislation that's been proposed out there that would allow the government where companies can, as I understand it, make their records secure to keep people from getting in.

Then there is some element that believes that the FBI ought to have the key to get into everyone's records. I guess that would scare me a little bit. I have the greatest respect for you, but whether that isn't a private property right.

What are your comments in that regard?

Mr. Gallagher. Perhaps a related concern, when we talk about economic espionage, how does that differ with just competitive sharing of knowledge or competitive interest?

The Economic Espionage Act put three elements into Section 1832, which is the traditional criminal aspect. There are two aspects of intent that are required in order to have a criminal prosecution.

One is that the individual had intended to convert a trade secret to the economic benefit of someone other than the rightful owner.

And secondly, and it has a big "and," and I underlined it, intended or knew that the offense would harm or injure the rightful owner.

And thirdly, that the individual knowingly engaged in this activity.

So Congress anticipated some of the concerns of where is law enforcement going with this type of legislation and recognized some of the individual rights.

There's another aspect of the statute that Mr. Torrence had pointed out, and that is there's a section, Section 1835, that orders to preserve confidentiality, that once a case is brought before a court, that the company, by virtue of a prosecution where they were the victim, don't, unfortunately, then give up their rights to the information that they were trying to protect in the first place.

So there has been some recognition already on the need for confidentiality and the need to protect individual rights of companies.

Mr. Torrence. If I may address the foreign aspect.

Whether a case is a national security traditional espionage case or a case brought under this law, economic espionage itself, when there is a foreign element, we frequently – I should say we usually – use the intercept techniques to solve those cases.

And that, of course, comes under court orders.

In our case, the Foreign Intelligence Surveillance Act. And my understanding of our request regarding encryption is that that would not change any requirement that we face today to conduct an intercept.

We still would be required, short of requesting nothing else, required to go to this court and have these intercepts approved.

So we're not looking for any broad, expanded capability, nothing but the same capability we have right now.

Representative Ewing. I think that's important and you clarified that, I think, very well.

The thing that was bothering me, if you had the right or the power to go in, the technical power to go in and invade someone's private files, you can't do that today without a court order.

If it's a paper file, you may know that there's something in that file that you have a right to have or needs to be brought forth. But that's our protection, that it's done through a court.

I was just concerned about whether this would give any law enforcement agency excessive power that might not be there today.

Mr. Gallagher. I think Mr. Torrence said it well. We're not looking for any additional power or authority.

Mr. Vatis. I think, in fact, what's happening now is that technology is threatening to undermine the established constitutional system that we have, because under that system, people's privacy is protected by the Fourth Amendment. But there are certain instances where if there is probable cause to believe a crime has been or is being committed, law enforcement is entitled to intrude into someone's private realm for the purpose of investigating criminal activity, but only upon a determination by an independent judge that there is such probable cause.

The technology threatens to undermine that system because a judge could find that there is probable cause to believe that a crime is being committed, issue a court order allowing us to do a search or an electronic surveillance, and then find that encryption prevents us from doing the search or surveillance.

So, in effect, the technology thwarts the order of the judge.

What we're trying to do is to make sure that the constitutional balance that we've constructed continues into this new technological age in which people use encryption.

And I want to stress that encryption is really a vital tool for individuals and businesses to protect their privacy. But we have to recognize the implications that the use of encryption by criminals and terrorists and other malicious actors has for law enforcement, because it does threaten to shut down some of our most effective investigative tools.

And so, we have to find some way of dealing with that adverse impact of the technology.

Representative Ewing. Thank you all. Thank you very much.

Representative Saxton. Let me just – Senator Robb, incidentally, has joined us and we're very pleased that he's here and he has some questions in just a minute.

But on the way to Senator Robb, let me just try to ask a question that is related to Mr. Ewing's line of questioning.

In simpler times, if we had secrets that we wanted to keep, in a general sense, we'd lock the door, keep people away that we didn't want to have access to the information.

The subject of locking the door relative to cyber-space, cyberism, is a different subject, isn't it? And encryption, as you just pointed out, is part of perhaps the answer to keeping people out.

But do we lock the door effectively today? Back in the days when we locked doors, we had people who picked locks.

Mr. Gallagher. Let me give you a very simple, direct example where locking the door is more complex.

We may lock the door to this room, but then I take home the laptop computer that allows me to be very effective, and that laptop computer is stolen.

And someone is able to break into that computer and, lo and behold, it has all the secrets of this room that we had just previously locked the door on.

And that's why, especially in the technology arena, the potential loss with the simple theft of a laptop computer or ability – U.S. industry depends very heavily on the World-wide Web and the use of the Internet.

And because of that, it's one large highway that you can enter into.

So locking the door has become such a more complex issue, the ability of criminals or terrorists or intelligence agents to enter into that highway and to get off and come into a room where previously, you're right, it was so simple early on just to put it under your pillow and sleep on it and it would be safe or lock the door and walk away and feel secure.

That doesn't exist today.

Representative Saxton. Thank you.

Senator Robb?

OPENING STATEMENT OF SENATOR CHARLES S. ROBB

Senator Robb. Thank you, Mr. Chairman.

I regret that I was not able to be here for the earlier testimony. There are other hearings going on simultaneously, and as we speak, I have a large group waiting for me in my office that I'm going to slip back to in just a moment.

But this hearing, and the general subject matter, have been an interest of mine for a long period of time.

I don't know whether it has been covered yet, but I'd like to ask a very basic question about the issue of encryption controls.

I know that the director has taken a strong position on this. I am also very sensitive to the need for our law enforcement agencies to be able to use whatever tools are available, and appropriate and legal, to intercept messages, particularly the kinds of messages that might have large-scale life or death consequences.

I can envision a number of consequences that would make it virtually imperative that we be able to interdict or intercept communications that might be carried on between criminal parties.

However, it's hard for me to make a distinction in my own mind between controlling missile technology and other dual-use technology, which we can justify controlling on the basis of security classification, and the simple ability for anyone to communicate, be they legitimate or criminal in terms of whatever purpose that they might have.

I've been debating this in both closed and open sessions, but there's nothing I'm discussing now that has anything to do with security classification.

If you have anything that you'd like to go into, and respond in closed session or for the record, I'd be pleased to receive it, but for the most part, I have a basic philosophical question.

And that is, why should we, in effect, restrict any manufacturer from the production of equipment that might be used to transmit encrypted information that would be criminal or have other unwanted consequences, simply because we want to reserve the right, under certain circumstances and with appropriate court order, to be able to go and break that encrypted message.

Again, I serve on the intelligence committee and the armed services committee and the foreign relations committee, so I deal with a lot of these topics. But the question I'm asking is more philosophical.

And that is, knowing the use to which encrypted material or encryption devices might be used, why should we in effect bar all

encryption devices that have a certain power or above, based on the belief that we might not be able to intercept in timely fashion, or at all, a criminal or terrorist-type communication?

What's the basis for that prohibition in a philosophical sense, other than our desire to want to maintain the ability to be one up on anybody?

Mr. Torrence. I can address that in generalities, Senator, maybe from one perspective. And mine is from the espionage perspective, and today, economic espionage, of which, certainly, in pure espionage, always, or generally always concerns foreign entities, foreign organizations. And the intelligence services and the foreign governments that we have confronted over the many years of this are very advanced in their techniques for stealing secrets.

Our ability to defeat that, to solve those cases, is heavily dependent upon electronic surveillance, again very carefully applied, probably with far fewer instances than the American public would think that we use.

I'm not addressing the terrorism aspect, but internationally, that would be the same issue. It's an international world and if devices are used by the services and we are not able to intercept certain communications, be it life or death or the communications between intelligence officers as an example, then it would be very difficult to solve these cases, in which highly trained people are involved in those, very, very highly trained people.

So I guess, simply, the international aspects of what the FBI does today is far greater than what it's done in the past.

So that's significant to us.

Senator Robb. Let me say that I understand all of that, and more, and I have been debating these with my usual co-conspirators to bolster our security capabilities, defense capabilities, et cetera, and our anti-terrorist activities.

But I have a problem with simply saying that if there is a device that, can be used to communicate for any purpose, that we ought to restrict the export of that device.

There are a lot of practical arguments that suggest that others can and will eventually provide the same kind of devices and may even leapfrog the technology that we can develop here if we constrain our own domestic production.

But putting that aside, I'm more interested in the broader question of why we should say, in effect, no one can be permitted to have a device

that gives them the power to communicate and keep their message secret from us, and using the most extreme example, communicate information that might be used to actually implement a terrorist attack.

I can put it in the most aggravated case and still have trouble with the philosophy behind it.

Mr. Gallagher. Senator, given the consideration of time today, maybe it would be best for us to have a representative of our congressional affairs office make an appointment to come see you direct and be able to discuss this in far more detail.

These are very sensitive, critical issues that I think we would be very interested in engaging in a dialogue with you very directly on this issue to resolve some of your concerns.

Senator Robb. I've had some of those discussions and again, I'm still grappling with the larger philosophical question, which does not go to any of the details.

Let me ask you, then, what kinds of cooperation has the FBI had with other agencies that might have similar concerns in addressing the whole question of cyber-crime, generally?

Mr. Gallagher. Let me first address cyber-banking because I think that is a good example.

With the significant potential impact of cyber-crime on financial institutions, with the significant growth of banking on the Internet, anticipated growth of banking on the Internet, the FBI, with the Department of Justice and the Department of Treasury, have created a cyber-banking working group.

The purpose of the working group, it brings together all the Treasury agencies, all of the regulators, and all of the Department of Justice law enforcement entities that are looking at this particular crime.

The goal is to raise the level of awareness of the potential of fraud using computers through the financial institutions and at the same time give some guidance out to the financial institutions and the regulators to increase the cooperation between the banking industry and law enforcement, to allow the FBI to receive the information that we rely on to begin an investigation.

In the banking industry, there is a suspicious activity report which is submitted any time a bank sees the first indication of a crime.

There is no aspect of the SAR or suspicious activity report, there's no box to check off to say, we think we've been victimized by a computer crime.

Computer crimes is a new phenomenon, relatively new in the United States. We need to educate the banking industry to be aware of the need to report these types of potential intrusions into this system so that the FBI can respond an work with them in order to prevent the loss if there is an emerging attempt, and at the same time, where we can, investigate and prosecute violations of law.

So we're working very aggressively in the cyber-banking arena.

Senator Robb. Mr. Torrence?

Mr. Torrence. In the economic espionage area, we of course work with all agencies in the intelligence community because economic espionage is so similar to regular espionage.

So we have ongoing relationships and regular discussions with those agencies.

We also helped establish in 1998 a working group called the Department of Defense Counter-Intelligence Science and Technology Protection Working Group, a very long title, but a group that includes all elements of the Department of Defense and us, in looking for ways to protect defense-related technology.

We also, in addition to training industry, which is a major part of what we do to implement this law, we have also interacted some with some friendly foreign intelligence services that have actually expressed an interest in this law – how does it work? – and they want to be informed of it.

So we've provided them similar type of discussions and information that might benefit them as well.

Again, it's an international area, so we do work with these friendly countries in this area.

Mr. Vatis. Maybe I'm a glutton for punishment, but I'll come back to encryption for a second because I think it addresses this issue as well.

I think we shouldn't think of encryption as an issue just of national security or counter-espionage; or that it's just foreign powers who would be using it.

I think we have to look at this also as an issue of domestic public safety because it doesn't impact just the FBI in its more esoteric activities.

It impacts the everyday law enforcement activities of the Drug Enforcement Administration in dealing with foreign drug cartels as well as drug dealers in this country.

It impacts state and local law enforcement in all the investigations that they conduct that involve electronic surveillance or searches of computers.

If you think about the cases that have been made over the years against drug cartels, against organized crime, those cases could not have been made if the telephone conversations that we were trying to wiretap were encrypted.

And I think today, in the cyber area, we've been talking about some of the more sophisticated means of using cyber-tools to attack an infrastructure or to rob a bank by shifting funds around.

I think even more mundane criminal activity now depends on computers for such simple things as keeping records of a criminal organization's activities or just common communications.

And so we are finding more and more that evidence resides in computers.

Well, if the stored data in those computers that we vitally need to make cases is encrypted in a way that it's unbreakable to us, again, it's going to have a serious impact not only on our regular, everyday investigations, but on the investigations conducted by the hundreds of state and local law enforcement agencies across the country.

And so, I think, philosophically, this is not just a national security issue and it's not just a commercial issue, but it's also a public safety issue.

So, if there is a way to have strong encryption – which is so critically important to businesses and to individuals – and allows us to protect our information and our communications – but at the same time, preserve law enforcement's ability to do its public safety mission, then we should really find that compromise.

Senator Robb. I don't want to argue that point with you and I would cede all of the concerns that you raised.

But it seems to me to be difficult to argue that "you can't develop a communications system, if we don't have a built-in advantage in being able to break that system."

In other words, "we're not going to accept the challenge of finding a new way to intercept communications or stored data or whatever the

case may be." We are going to say, "you can't even develop, the technology can't advance," that would be the bottom line, I suppose, "unless we have a built-in advantage."

I have some difficulty with that argument. But, again, this is not the first time that I have had an opportunity to discuss this.

Could I ask one more question, Mr. Chairman, and then I am going to have to run, and I thank you very much.

In terms of estimating the cost and likelihood of any attack on our information technology infrastructure, how does the National Infrastructure Protection Center prioritize potential electronic threats and balance the cost of these threats against the cost of preventing them?

Cost-benefit analysis 101.

Mr. Vatis. I don't think we have any really good estimates of the costs that are imposed by cyber-crimes or attacks on the infrastructures, partly because we don't have confidence that all of the intrusions that are out there are being reported to law enforcement by industry yet.

And, as we talked about earlier, there are some types of intrusions that are really impossible to quantify in monetary terms.

But we do see a very broad range of threats, ranging from the insider to the recreational hacker to the organized crime group to terrorists.

Senator Robb. But it seems to me, within the group you could establish some higher likelihoods and with the five hackers that have gotten a lot of publicity here in the last couple of weeks, establish that hackers provide, say, more of a threat than some other type of intervention in various other secure means of communication.

Mr. Vatis. I think in terms of the number of cases that we see, most of the cases probably involve insiders and hackers within the United States.

But I think in terms of the magnitude of the threat, the more serious threat has to come from foreign hostile nation-states, foreign intelligence services, and terrorists because their intent and their motivation is to cause much more serious damage.

Those are fewer in number, probably, but the magnitude of an incident that involves one of those threats is obviously going to be much greater.

Mr. Gallagher. Senator Robb, maybe in an effort to quantify it, there was a 1996 study by the American Society for Industrial Security

that cites that the high-tech industry has an average loss per incident of intellectual property loss of approximately $19 million per incident.

That's not an FBI study, but it begins to put a dollar figure on the table as to the potential impact of intellectual property loss.

Senator Robb. Okay. Mr. Chairman, I have exceeded my time and I thank you very much for the opportunity.

Representative Saxton. Senator, thank you very much.

Mr. Gallagher, I believe it was in your opening statement, you mentioned a very dramatic increase in cyber-banking. I believe you indicated that there was something like a 600-percent increase over—

Mr. Gallagher. Anticipated increase over the next two years. And there are approximately 1100 banks on the Internet. The vast majority of them are existing banks that use the Internet for advertising purposes. But we're beginning to see some transactional capabilities over the Internet.

Representative Saxton. Now what does that say to us about the opportunity for theft, the opportunity for hacking into a system and creating a nuisance or creating a situation – is there a 600-percent increase, I guess is what I'm trying to ask, in opportunity to do bad things?

Mr. Gallagher. Fortunately, the United States banking industry is a very sound industry with a lot of regulations overseeing it and a lot of very well-disciplined structure to it.

However, I think you have to look at it as not only attacks on the banking industry.

One of the by-products of criminal activity is money-laundering. If you envision – and again, you used the term earlier, it used to be a lot simpler when we could just lock the door and lock the secrets in.

It used to be if you had a money-launderer, you would have to take a suitcase full of money and try to transport it outside of the United States.

That's not the case today. If you can get on transactions over the net and move money around the world, envision the organized crime element or the drug cartel that wants to launder money and be able to move money very quickly and dramatically.

It just creates a whole new area of potential criminal activity that will be facilitated by some of the benefits that we desire. And that's the benefits that we have become accustomed with with the Internet.

Representative Saxton. Thank you. Mr. Vatis, with the dramatic advances in technology, are you able to keep up with these increases in terms of the training of your staff?

Do you need more tools? Do you need more resources? I guess that perhaps is the question that usually elicits a yes answer in government circles.

(Laughter)

Mr. Vatis. Yes, absolutely. I think our two most critical needs right now are in the areas of personnel and equipment, and particularly personnel.

I think there have been recent studies that indicate that the private sector has a severe shortage of technically proficient employees in this area as we continue into the Information Age.

And I think we also suffer from that same shortage, particularly at the government pay scales. It's difficult for us to attract the people with the really advanced computer skills that we need in order to conduct these very high-tech investigations.

On the equipment side, we also have a problem in that the technology advances so quickly, that it almost seems as though each investigation we conduct requires some new tool because the technology that's involved has changed.

And so, it's not the case that we can do an investigation, build a new tool in order to trace an intrusion back to the intruder, and then put the tool on the shelf and bring it down for the next case.

The next case almost inevitably involves some entirely new technology that we need to build a new tool for.

So we need to have a lot of flexibility and also, I think the technical wherewithal and the scientists to help us build these tools on a continuing and evolving basis.

Representative Saxton. And on the personnel side, do you have the expert folks working for you?

Do you have to go outside and contract out for services from time to time?

Mr. Vatis. We do, and I think Mr. Gallagher referred to that in the 911 case as an example. I think we rely a tremendous amount on contractors now because they have a lot of the expertise.

And that's one of the things that we're trying to do with the Center, is build more of the expertise in-house at FBI headquarters, but also, critically, out in the field offices because that's where the investigations are conducted, in the 56 field offices.

We need the expertise really throughout the country.

But that is a big recruiting issue that the FBI as a whole is facing right now.

Representative Saxton. Thank you very much.

Mr. Ewing, I don't know if you have other questions.

Representative Ewing. (Nods in the negative).

Representative Saxton. I think that we have kept you here for quite a long period of time, and we appreciate very much your sharing this information with us and your area of expertise is obviously very well developed.

We are pleased, obviously, that not only you were here, but that you're doing the kind of a job that you are doing.

So thank you for being with us this morning. We're going to keep the record open for a short period of time so that other Members who may not have been able to be here this morning may want to submit some questions to be answered in writing.

Thank you very much for being with us this morning. I thank Mr. Ewing also for hurrying back from Illinois to take part in this morning's hearing.

We appreciate that very much.

At this point, unless there is further business, the hearing is adjourned.

Representative Ewing. Thank you, Mr. Chairman.

Mr. Gallagher. Thank you.

Mr. Torrence. Thank you.

Mr. Vatis. Thank you, Mr. Chairman.

[Whereupon, at 12:00 noon, the hearing was adjourned.]

SUBMISSIONS FOR THE RECORD

PREPARED STATEMENT OF REPRESENTATIVE JIM SAXTON, CHAIRMAN

The hearing this morning is on cybercrime, transnational crime and intellectual property theft and, in particular, the role the Federal Bureau of Investigation plays in this arena.

Cyberbanking is now a growing part of our everyday lives. The information is easy for us to use, but it is also vulnerable to tampering and theft.

The proliferation of technology has increased the opportunities for conducting economic espionage. The theft of trade secrets has caused billions of dollars in losses.

Foreign governments actively target U.S. companies and the U.S. government in order to steal our capital technologies and information.

To begin to better understand these emerging economic and national security threats as a first step we have three knowledgeable gentlemen from the FBI with us today: Deputy Assistant Director Neil Gallagher, Criminal Division, Deputy Assistant Director, Larry Torrence, National Security Division; and Deputy Assistant Director and Chief Michael Vatis, National Infrastructure Protection Center.

I would like to hear the testimony of each of you and then go to a question and answer segment.

Intellectual Property Theft Economic Analysis Case Study

April 1997

Project Manager:

S.W. Martin

Contributors:

D.E. Deonigi
K.A. Freund
J.A. Jaksch
J.M. Roop

This work was supported by the Federal Bureau of Investigation under a Related Services Agreement with the U.S. Department of Energy (DOE) under Contract DE-AC06-76RLO 1830, Purchase Order Number A605214. Pacific Northwest National Laboratory is operated for DOE by Battelle.

Case Study

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC06-76RLO 1830

For further information please contact
Scott C. Williams, Supervising Special Agent, Economic Counterintelligence Unit, Federal Bureau of Investigation,
Ninth Street and Pennsylvania Ave. N.W., Washington, D.C. 20535,
Phone (202) 324-4276.

Case Study

Executive Summary

The Pacific Northwest National Laboratory has developed a methodology and undertaken a case study on the theft of intellectual property (IP) at the request of the Federal Bureau of Investigation. The case, revealing information disguised for the purpose of the report, relates to the IP embodied in the product of a U.S. manufacturer. The analysis assumes that the IP, legitimately incorporated into a proposal to a foreign government by the U.S. firm's foreign licensee, was transferred without authorization to a third party foreign competitor during competition to supply products to the foreign government market. It should be noted that the U.S. firm's foreign licensee and the third party foreign competitor are closely aligned with the foreign government which solicited the proposal. In the end, the third party foreign competitor was awarded the contract in question. Two scenarios have been established to measure the economic impact of this theft.

The analysis compares the economic impacts of the theft of IP relative to a base case in which it is assumed that absent any IP theft, the foreign licensee wins the bid. In addition to the immediate consequences of losing the bid, this scenario assumes that in the future, the foreign competitor captures market share from the U.S. firm, especially in foreign markets. Losses are estimated by comparing the theft case to the base case. Two separate scenarios were analyzed, each with a base case and IP theft case.

The first scenario assumes that the IP was transferred to the foreign competitor before the bid ("Pre-bid" scenario) and that in consequence, the U.S. firm's foreign licensee lost the bid. The direct impact of this theft of IP over the period 1992 to 2005 would be:

- Loss of domestic sales of $147 million
- Loss of foreign sales of $488 million
- A cumulative reduction in the U.S. trade balance of $714 million
- Lower tax revenues to Federal, state, and local government of $129 million
- A loss of jobs by the U.S. firm equivalent to 2,600 full-time-year equivalents
- A loss of 9,542 job-year equivalents for the economy as a whole.

Figures ES-1 and ES-2 summarize the impacts of this scenario. The impacts that occur as a result of the IP theft are shown in Figure ES-1. The loss of royalties occurs in the period 1994-1998, when the foreign competitor provides products to the foreign market as a result of winning the contract over the U.S. firm's foreign licensee. The profits from the sale of these products are the largest component of the company's loss, but unpaid taxes, shown as a savings to the company (above the

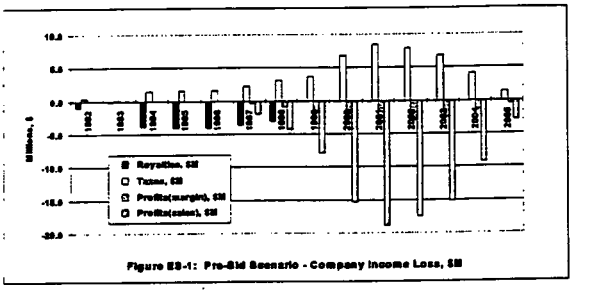

Figure ES-1: Pre-Bid Scenario - Company Income Loss, $B

Case Study

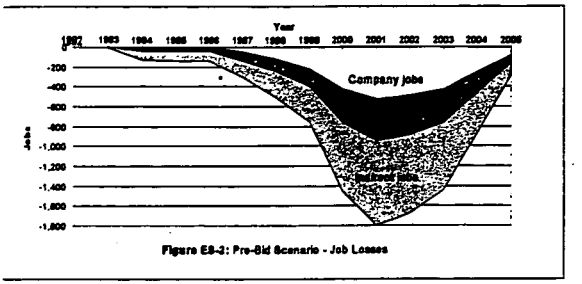

Figure ES-2: Pre-Bid Scenario - Job Losses

zero axis), also are a substantial loss to both the state and federal governments. The employment impacts of the IP theft are shown in Figure ES-2. Job losses reach a total of about 9,500 over the period to 2005, and these are shown in three categories: company, suppliers, and indirect jobs. The company loses jobs directly, as do the suppliers that provide the parts and materials to the U.S. firm. The rest of the economy also loses jobs as a result of the losses to the U.S. firm's suppliers. Despite the losses, the analysis shows that the company would remain viable.

A second scenario ("Post-bid" scenario) assumes that the foreign competitor won the bid legitimately, but that the unauthorized transfer of the U.S. firm's IP to the foreign competitor occurs afterwards. The direct impact of this scenario is a two-year delay in the development of the competitor product. The two-year delay was estimated based on the development time for the U.S. developed product and the foreign competitor's product. It took the U.S. firm 7 years to develop the original version of the product, while it took the foreign competitor only 3 years. Two of the foreign competitor's 4-year advantage is attributed to the IP theft. The fact that there is a 2-year delay in the foreign competitor's entry into the foreign and U.S. civilian markets reduces the impacts. The main loss of sales in this case is also in foreign sales, but the relative losses are less -- only 71% of the first scenario. Domestic sales are virtually unchanged in this scenario at 82,589 units, compared with 83,226 units in the first scenario. Job-year losses through 2005 under this scenario are about 8,178, compared with roughly 9,542 lost job years under the first scenario.

Sensitivity analysis is used to examine the importance of major assumptions to the results of this case study. This sensitivity analysis shows that the results of IP losses are not highly sensitive to the assumptions we used. If the foreign competitor captures 25% of the foreign markets and U.S. civilian market (rather than the 50% forecasted), then the U.S. firm's net income would increase by only 12%. If the foreign competitor captures 75% of the market, the U.S. firm's net income would be reduced by 14%.

The major lessons learned fall into 2 categories--lessons from the case study that could apply to U.S. business in general, and lessons learned in the process of undertaking this project. These lessons are summarized as follows:

- It may be in the interest of public policy to strengthen U.S. laws to protect designs from exploitation.

Case Study

- U.S. companies should not assume that foreign businesses or governments will give U.S. proprietary information the same level of protection as that provided by the U.S. Government.
- U.S. companies might consider whether it is worth the risk to share their IP with foreign companies if this IP is expected to have a long product life cycle and cannot effectively be protected.
- Cooperation of the alleged injured party in sharing data and information is critical in estimating the impact of IP theft.
- Project analysts found that market analysis was the most effective method for evaluating the impact of IP theft.
- Collateral data provided by the FBI can make a difference on the number of assumptions made during the analysis.

The developed method appears to work well in the case study undertaken. Nevertheless, a question remains about its general applicability. To explore this question, we examined the case of the theft of radar and electronic countermeasure technology from Litton Systems by a Korean company, Ssangyong. Court documents were used to construct the events surrounding this theft. These documents also provided much of the financial information needed to assess damages; this information is very similar, though not as detailed, as that needed to estimate IP theft under the methodology used in this case study. While we did not apply the methodology rigorously to this second case, indications are that the method would likely apply.

Contents

Appendices

Case Study

I - Introduction

At the request of the Federal Bureau of Investigation (FBI), the Pacific Northwest National Laboratory has developed an analytic framework to examine the economic impact of theft of intellectual property (IP) from a U.S. company. PNNL then undertook a case study on the loss of IP embodied in a U.S. manufactured product. While this report contains sufficient information to allow an understanding of the methodology, the specifics of the case have been made generic to protect the victimized U.S. firm. The framework sets up a method to determine the impact of theft to the company whose IP is stolen, as well as to its suppliers and the nation. As originally proposed, the project would focus on the development of a method for evaluating the resultant impacts of the theft of IP and then apply the method to one or two case studies. While a second case has been examined, the methodology has not thoroughly been tested against a second case study to determine if the method is generally applicable.

The case study assumes that the IP, described in a proposal by the U.S. firm's foreign licensee, was transferred to a third party foreign competitor during competition to manufacture and deliver products to a limited foreign government market. The IP believed to be transferred consisted of technical drawings and other specifications of the U.S. product. It is thought that the foreign competitor used the U.S. firm's IP to win the contract, eventually delivering a product very similar to the original U.S. design. This case study examines the economic impact of IP theft to the nation, the U.S. firm and its suppliers in terms of:

- Lost jobs
- Taxes
- International trade
- Lost revenues
- Lost income
- Profits.

The U.S. firm was extremely cooperative in providing us with data to do the analysis for the case study. They not only provided us with historical market, employment, and financial data, but they also provided product definition. It would have been nearly impossible to conduct a plausible analysis on this case without their willingness to provide detailed information.

This report consists of five chapters: Introduction, Methodology, Case Study, Applicability of Methodology to Other Cases, and Lessons Learned and Recommendations.

Chapter II, Methodology, describes the framework developed to conduct the economic impact analysis, including how to develop a base case against which IP theft can be compared. This section also describes the type of data necessary to assess the impact of IP theft.

Chapter III, Case Study, provides a brief history of the case being analyzed, an assessment of the value of the IP stolen, and a discussion of the impacts of the IP theft to the nation, the company, and its suppliers. Details on how the future market size was projected under both a base case and IP theft scenario are also provided. The results of the impacts from IP theft are presented in terms of lost sales, jobs, profits, tax revenues, and trade volume. Note that it is not the intention of this

report to analyze the case itself, but rather to assume IP theft, and to analyze the economic impact of this IP theft.

Chapter IV, Applicability of Methodology to Other Cases, briefly considers a separate case, recommended by the FBI, to test the methodology described in Chapter II to see if it would be applicable to other cases. This chapter relies only on information provided by the FBI. No additional information was collected from the parties in the case. Therefore, this analysis provides only a cursory application of the methodology to a second case.

Chapter V, Lessons Learned and Recommendations, describes the lessons learned and recommendations made about the process of analyzing the impact of IP theft, as well as lessons learned or questions raised about the case study that should generally be applicable to U.S. business.

II - Methodology

Economic analysis of the theft of IP requires that a framework for analysis be defined, that the framework be applied to a case in point, and that alternative cases be examined to ensure that the framework is amenable to general application. While the framework has been defined and applied to one case study, we cannot claim that the method is universally applicable. To make that claim, the methodology would have to be repeatedly applied to a variety of case studies, which has not yet been done. A second case is described in Chapter IV, but does not qualify as a case study because the methodology was not rigorously applied.

Nevertheless, this section does define a framework and describes how it can be used to establish a base case against which the IP theft case can be compared. The theft case will then be explained, and information and data requirements will be enumerated.

Analytic Framework

The theft of IP robs an individual or corporation (referred to hereafter as the company) of the ability to reap economic rewards from that property. Determining the impact of that theft requires the construction of at least one hypothetical case that compares the scenario of IP theft and market exploitation with what the market situation would have been for the IP owner absent the theft. Alternatively, if the theft occurred, but no market advantage was taken of the property, a case must be constructed in which advantage ***was*** taken. For example, for a company that has possession of stolen IP but has not yet used it in the marketplace, it would be necessary to construct a case in which the IP was used to the company's market advantage. It should be understood that since any estimation of likely consequences requires that some hypothetical case be constructed, these hypothetical consequences may never be precisely correct.

In the arena of legal combat, adversaries will take advantage of this ambiguity to exaggerate the impacts (or lack thereof) of the theft. One of the objectives of this analytic framework then, is to outline what is reasonable to include and exclude in such an analysis, in order to put bounds on the magnitude of the impacts.

These impacts will normally focus on the company, the geographical region and the economy and will relate to the economic health of affected entities or areas. Types of measures normally considered would include the profitability of the company, the dislocation impacts to the region, or the employment changes for the country as a whole. The magnitude of the economic impact can be assessed through sensitivity analysis -- by considering ranges of possible outcomes and perturbing the analysis so that consequences vary, one can determine the assumptions that are most sensitive to the conclusions that are reached.

How the actual and hypothetical cases are constructed will depend on the extent and availability of data, but will generally make use of the following information:

- Economic data related to the company. What are the profit margins at different levels of production? What are the relevant costs -- labor, materials, capital? Is this one of many products that this company sells? Is it a typical sized company in this industry? What is

the financial health of the company? How profitable is the product and how many jobs depend on sales of the product?

- Other related economic data. What is the extent of the market for the product? Who are the major suppliers and where are they located? What industries are major suppliers? How important is this industry in the regional and national economy?
- Understanding the origin of the intellectual property. How is the product manufactured and how complex is the process? What is the product life-cycle of similar products? What portion of the product, if any, is protected? What R&D went into the product and how was it financed? How difficult would it be to reverse engineer the product? If the product is not patentable, could it be protected by copyright or registration or other means?
- Characterization of the product that embodies the intellectual property. What are its sales? What market share does the product hold? What competitors produce similar products? How is pricing determined? What is its special market niche? How is it classified in trade? How complex is the market in which this product competes?

With this information, and related information about the competitive advantage derived from the theft of intellectual property, both a base case and an alternative case can be constructed. We will discuss these two cases in turn, then address issues of data and information collection.

The Base Case

The base case establishes what would have happened had no IP theft occurred. For expository purposes we will assume that the IP is embodied in a product (although the analysis would not be greatly affected if, instead, the IP were embodied in a service). The first step in the analysis is to characterize the product and how it is manufactured. In addition to this information, we need to know something about the intellectual property, how the company fits within its market niche, and other economic information about the company. This information applies not only to the base case, but also to the alternative(s).

This case then is compared with the alternative (or multiple alternatives) that shows the likely events after the theft of the IP.

The IP Theft Case

Most IP has a useful lifetime bounded by the law, the market, and control of any trade secret. The U.S. patent system offers 17-year protection, but the market usually moves to another technology faster. The impact as a result of the loss of IP to a foreign competitor could be the loss of sales both domestically and abroad, reductions in employment both to the affected industry and to suppliers, and consequent reductions in income, profits, and shareholders' wealth. These impacts can be reasonably assessed if adequate data are available. Intellectual property value is discussed in more detail in the case study (Chapter III).

Case Study

Data and Information Collection

The discussion above has been extremely generic. This section, still in generic terms, describes what information is needed to construct a base case and alternative cases. The data fall into the following four categories: product sales, other economic data, data about the IP itself, and data about the company.

Product Sales

The product's unique features are what provide it a market niche. Understanding this niche allows the projection of market shares and estimates of future sales. For an estimate of sales, the market may need to be segmented to capture the differences in competition that the product may face: for example, foreign competition may be much more severe in sales outside the domestic economy than within it, or there may be certain market niches that are more difficult to penetrate than others. Expectations about future sales may be provided formally, as part of the corporate planning process, or may be done informally, based on rules of thumb. Once sales are established, attention can be turned to other relevant economic information.

Other Economic Data

More information than that about sales is needed to determine the impact of the loss of IP. To determine the total impact on the company, we also need to know how a unit sale translates into employment and other impacts. For this we need to know margins -- how much of the revenue of a sale covers costs and how much is profit for the company. This may vary, depending on the volume of sales and the way overhead costs are allocated to, or vary with, sales. A unit sale will have different impacts, depending on whether the company manufactures the components that make up the product or purchases these from other suppliers. And it is also important to know how much of the supplied material is "off-the-shelf" components that could be obtained easily and how much of the materials are custom-made for this product alone. Intellectual property embodied in a product that is designed to meet certain performance specifications but is made up of off-the-shelf components may be more difficult to protect than a product that is made up of highly specialized components. This suggests the need to understand the nature of the intellectual property.

Understanding the IP

If a product is successful, it will be emulated. The performance of a highly complex piece of equipment, such as an automobile or a computer, can be reverse engineered to provide much the same performance as the highly successful first entrant. The Polaroid camera, the IBM Personal Computer (PC), and the Chrysler minivan are excellent examples.

These examples also point out the differences in ability to protect IP. The Polaroid camera was effectively protected, worldwide, by patent protection, excluding its replication for 17 years after its development. IBM's first personal computer was pieced together using readily available, off-the-shelf components except for one vital board that IBM protected by copyright. When Compaq reverse-engineered that component, it was done in such a way that there was no violation of the

copyright and hence no legal recourse. This opened the PC market to a startling array of competitors. The minivan, although a unique design, was not directly protectable. Instead, Chrysler grabbed the lion's share of that particular market niche. Although all major automotive manufacturers had competing vehicles within one or two years, Chrysler protected that market niche solely through continued innovations and improvements to the product.

For many products, then, there is the expectation that similar products will eventually find their way into the marketplace to compete with these successes. Many factors will affect how that emulation will occur. The cost of reverse engineering of the product is one factor, as is whether the company does its own research and development. The second factor is the extent of the market and whether it is possible for more than one competitor to prosper (or survive) making this product. A third factor is the extent to which the IP is protected by law -- patents, copyrights, etc.-- and the extent to which the owner of the IP could collect damages for its theft.

Understanding the Company

With other information in hand, we can use these data to assess the company and the possible impacts of the theft of IP on the company. In addition to the information about the product, the IP and other economic information, we also need to know how diverse the company is, what its market strength is relative to the competition, and how effectively this company can exploit the IP under examination.

With this set of data, a base case and one or more alternatives can be examined. In the next two sections we describe the dimensions of the impact and how these impacts are estimated.

Dimensions of Impact

The theft of intellectual property will, perforce, affect the injured company. If the thief is domestic, there may be little, if any, impact on the economy as a whole, although there may be regional impacts if the companies are located in different geographical areas. If a foreign company steals the IP, we could expect national impacts in areas such as

- U.S. jobs
- U.S. federal and state tax revenues
- U.S. exports and imports.

Both the affected company and its major suppliers will be considered for the analysis of the impact on U.S. business as a result of the IP theft. In addition, these initial impacts will reverberate throughout the economy and further impacts may also be important. Specific factors to be included in the impact on the directly affected companies include

- Market share, domestic and worldwide
- Revenues as a result of product sales or royalty payments
- Profits and shareholders' wealth

Case Study

- Direct employment to the company and its major suppliers
- The viability of the affected company(s) and the products that incorporate the IP.

Central to these impacts is the loss of sales.

Estimating the Impacts

Much of the analysis rests on forecasts of sales of the product that incorporates the IP. Consider the IBM/Compaq case mentioned above. IBM had forecasts of PC sales that it anticipated under the expectation that its IP would not be replicated within a reasonable time frame. It failed to reach these sales expectations precisely because Compaq sales substituted for IBM sales. As a result of this loss of market share, IBM sold fewer units; this probably reduced the profit per unit as well. (The reasonableness of these IBM sales forecasts might be compared with the actual sales of all IBM, Compaq -- and other -- PC sales, but this can only be done after the fact.) By understanding the PC market and how price sensitive IBM's product might be to competition, this loss of market share could be anticipated.

From the loss of market share, a revenue loss could also be forecast and these revenue losses translated into reductions in profits, shareholder wealth, and employment for both IBM and the suppliers of PC components. Since IBM is the world leader in the computer market, the viability of the company and the PC were not challenged. Since Compaq was also a domestic company, the national impacts would be anticipated to be quite small, maybe even positive as a result of the direct competition with IBM. But if Compaq had been a foreign company, the impact of the (in this case, legitimately) lost IP value could also be assessed, through loss of domestic production, loss of jobs, and possible consequences to the balance of payments if these products had been imported rather than produced domestically. Both the sale of the product and the income generated through its production provide tax revenues to federal, state and local governments, so these impacts also could be estimated.

To determine national impacts that might result from lost production, two alternative approaches could be used. The first and more difficult is to employ a dynamic model of the economy, for which a variety of models are available. The Wharton Group and Data Resources, Inc. are the most widely used such models. The more reasonable approach is to use a static representation of the economy and apply well-used economic impacts tools such as input-output analysis. That is the approach taken here. In the case study that follows, we have used a model called the Sectoral Energy/Employment Analysis and Data System (SEADS-PC), which allows the examination of the impact of a loss of sales on energy use and employment for 85 industry sectors of the economy and for the economy as a whole. This model was selected based on its availability and familiarity to the analysts. The model is based on the 1987 Benchmark Input-Output (I/O) table of the U.S. economy.

The loss of sales to a particular industry can be translated, using such a model, into job impacts on the affected industry and for all other industries within the U.S. economy. First the sales losses derived from the case study are translated into 1987 dollars, then these lost sales are subtracted from the total of all sales in that industry also in terms of 1987 dollars. By translating all financial data into 1987 dollars, the sales losses derived from the case study can be subtracted from the

Case Study

total of all sales in that industry. The employment that results is compared with the base case (i.e., no sales lost) to see what the overall impact is for the economy and which specific industries, including the affected industry, are hurt by these lost sales.

As with the IBM example, these impacts could be applied to almost any circumstance. In Chapter III, we apply this approach to a specific product and company with the evidence we have collected that suggests the likely theft of the company's IP. The case study certainly shows that a foreign competitor replicated the design features of the domestic product. In Chapter IV we briefly examine an alternative case to see if the approach may have general applicability to other IP theft cases.

III - Case Study

Background and Time Line

In the 1980s, a U.S. manufacturer entered into an agreement with a foreign firm to bid on a contract to supply their product to a foreign government. Part of the arrangement was a licensing agreement, which included a written understanding that the information related to the technical know-how on how to build the U.S. product was proprietary. The agreement included a package of technical data comprised of engineering drawings, tooling drawings, and process sheets for all components, assemblies, and parts fabricated by the U.S. firm; engineering drawings of all components, assemblies, and parts purchased by the U.S. firm from outside suppliers; and other specifications for parts, where applicable. The agreement also provided for related engineering/marketing advice from the U.S. firm to their foreign license.

Essentially, the foreign licensee's interest in a licensing agreement with the U.S. firm was to develop a new product line embodying and/or utilizing licensor's technology, and to be able to include certain components embodying or utilizing licensor's technology in certain products which would not compete with the U.S. firm.

As part of the Licensing Agreement, the licensee agreed to pay a license fee to the U.S. firm of $1 million up front, and another $1 million if and when the licensee was awarded the contract. The licensee also agreed to pay a royalty of 4% of the Royalty Base for all licensed products sold, leased, or otherwise disposed of, on behalf of the U.S. firm.

During the proposal and bidding process, the foreign licensee indicated to the U.S. firm that their specs and performance were among the top of the producers, and that the competitors' proposed specs and performance did not meet the foreign government requirements. Final specifications and requirements were to be announced in the late 1980s. Unfortunately, by that time, the U.S. firm learned that a foreign competitor was proposing a product very similar to the U.S. product.

In the late 1980s, three of the original bidders on the proposal dropped out. It was at this time that the foreign licensee, as part of the bidding process, disclosed the U.S. product's package of technical information to the foreign government. Later that same year, the U.S. firm learned from their foreign licensee that a foreign competitor had won the contract.

The foreign licensee informed the U.S. firm that the reasons for losing the bid were as follows:

- The specifications were "changed."
- The price "objective" was 1.5 times the price of the winner and the winner's price was 10% lower that the best price the foreign licensee could offer.
- It was learned that the technical performance comparison was done by computer simulation. No actual test and evaluation was carried out.

After only two years, the foreign competitor who actually won the contract, revealed a product which was very similar to the U.S. product. Based on the complexity and high cost of the design process, and the relatively short development time for the prototypes to appear, it is believed that

Case Study

the foreign competitor used the proprietary technical documents which the U.S. firm provided to their foreign licensee partner, who in turn provided them to the foreign government, to help develop the prototype. It is not known how, when, or by whom such information was transferred.

Approach to the Case Study

We lack several pieces of information about the case that would have been helpful in building our loss estimates. Because of the missing information, it is necessary to make certain assumptions. We are assuming that the foreign competitor had access to the U.S. firm's intellectual property and used this IP to help develop a the prototype product. But even assuming they had access to the U.S. firm's IP, we do not know when the transfer took place. Was it obtained before the initial contract bid evaluation, or after the contract was awarded to the foreign competitor? We also do not know what recent and current actions have been taken by the foreign competitor to pursue foreign government and civilian markets. We also do not know what kind of agreements might have been reached in the future between the U.S. firm and their foreign licensee for pursuing markets, had the licensee won the contract. Because we have incomplete information, it is necessary to construct two separate scenarios, using different assumptions in each scenario. The first scenario assumes that the foreign competitor had access to the IP before the bid evaluation. The second scenario assumes that the foreign competitor won the bid on its own merit, gaining access to the U.S. firm's IP after the contract was awarded, however, allowing them to build the prototype and enter the market faster than they would have without the IP. Under both scenarios, the base case assumes that there was no theft of IP.

Scenario I : Pre-Bid IP Theft

Base case:

The agreement between the U.S. firm and their foreign licensee permitted sale of products in a specific foreign market defined by the contract being bid. The foreign licensee was required to receive permission from the U.S. firm prior to pursuing any other markets where they would be in competition with the U.S. firm. Since we do not know what, if any, markets the foreign licensee might have pursued should they have won the contract, nor do we know if any additional royalty agreement would have been signed, we are assuming for the base case that the foreign licensee won the contract and supplied only that market specified in the contract. Because of the small size of the market, we have also assumed that a company would not try to enter the market for these products without some guaranteed market. Because the foreign competitor does not win the contract under the base case, we are assuming that the foreign competitor would not have entered the market.

Property loss case:

Under this scenario, the foreign competitor wins the bid at least in part due to their use of the U.S. firm's IP. The initial loss to the U.S. firm is the $1 million license fee due to the U.S. firm from the foreign licensee upon winning the contract, and the royalties that would have been earned from those sales as well as sales of parts. In addition, as result of having the IP, the

Case Study

foreign competitor is able to enter the foreign markets faster than it would have without the benefit of the U.S. firm's IP. Therefore, in addition to the loss of royalties and spare parts sales, the loss will also include the U.S. firm's loss of sales to foreign markets. The loss of market share, therefore, will be based on the market share the foreign competitor is expected to acquire with the advantage of the U.S. firm's IP, compared with the market the foreign competitor might have been expected to acquire if it had no unfair advantage.

Scenario II: Post-Bid IP Theft

Under this scenario, the transfer of the U.S. firm's IP to the foreign competitor takes place after award of the contract. It is assumed under this scenario for both the base case and the property theft case that the foreign competitor wins the contract legitimately, based on price and/or other qualifications.

Base case:

It takes the foreign competitor 2 years longer to develop the product and enter the market under the base case than under the IP theft case, because the foreign competitor does not have access to the U.S. firm's IP. (See Intellectual Property Value, below, for a discussion of the 2-year market advantage.)

Property theft case:

The foreign competitor is able to enter the market 2 years earlier than would have been possible without the U.S. firm's IP. Under this scenario, the loss to the U.S. firm includes any losses in foreign market share (excluding the initial contract sales) that may have been lost due to the transfer of the U.S. firm's IP. Under this scenario, there is no loss of royalties or spare parts, because we have assumed that the foreign competitor won the contract legitimately.

Intellectual Property Value

To determine the losses relative to the base case, it is necessary to understand the value of the IP that was stolen. Intellectual property is valued in business and the courts in four basic ways: 1) research and development investment; 2) the willingness of others to pay for the rights to the IP (i.e. licensing); 3) the cost to produce a product with like features (i.e. reverse engineering); and 4) market loss to illegal copy.

The product life of most IP is determined by the law, the market, and control of relevant trade secrets. Although the U.S. patent system offers 17-year protection, typically the market moves to other technologies faster. Product life for this specific product is in the 10-to-15 year range. Look-alike copies of successful products are usually in the market within 2 or 3 years. For this study we have set the product life at about 15 years, and selected a time ranging from 1989 - 2005. During the last five years 2000-2005 the value of the design package will decline as various components are replaced by new advances not related to the original IP. During the final five years and after 2005, we assume that the technology change is followed by a still better product to meet ever-changing market needs. Sales by the U.S. firm will continue to be made and

Case Study

the company may prosper, but the product will contain few of the design features contained in the IP theft. The reduction in IP content is assumed to drop from 100% in 2001; to 80% in 2002; 60% in 2003; 30% in 2004 and 10% in 2005.

It is important to understand that no U.S. or foreign patents were filed for or approved for any elements of the product design. The following sections discuss several different methods for IP valuation and the IP values estimates for the product.

Development Cost

The development of the design began in the late 1970s, and within a year the U.S. firm delivered the first prototype product. The cost associated with this proof of concept in 1995 dollars was $4.537 million.

The second phase of development took two more years, during which time several additional products were produced. The cost of this phase in 1995 dollars was $36.885 million.

The third phase included final design, continued testing, manufacturing start-up support, and operating manuals. This activity cost $70.774 million in 1995 dollars.

The total development cost over 7 years, in 1995 dollars, was $112.196 million.

The IP contained all of the component drawings for the product. This was in fact the material provided to the foreign licensee under the Technical Assistance and License Agreement.

Other market versions of the product took 2 additional years to develop, at an additional cost to the U.S. firm of $19.2 million. In addition, another $20 million was invested in capital equipment. Again, no patent applications were made out of the development in at least 7 product variations.

License Agreements

Another method of valuing IP is by determining what the market is willing to pay for the right to the property. In this case the property was contained in the drawings and other technical data. The foreign licensee signed such an agreement with rights limited to serving specific markets.

The agreement provided for a payment to the U.S. firm of $1 million on signing of the agreement, plus an additional $1 million should the foreign licensee win the contract, and a royalty payment of 4% of the value of all future sales. A maximum was set on the total royalty payment of products of $25 million. In addition, at least $6,000 worth of goods and services would be purchased from the U.S. firm with each unit sold by the foreign licensee.

This agreement applied to a very limited market. The expected sale was 20,000 items over a 10-year period. The exact price that would have been paid for the products is not known. However, using the U.S. 1995 average price of $51,000 for the basic product, the sale of 20,000 units would be worth $1.02 billion. The royalties from such a sale would be $40.8 million. In this case the $25 million maximum would control.

Case Study

Thus the total value of the licensing agreement may have been $2 million for up front payments, $25 million in royalty payments, and about $20 million profit from the sale of goods and services, (assuming a $1,000 profit from each $6,000 sale). ***This totals $47 million as the maximum from the market specified under the Technical Assistance and Licensing Agreement.***

In the special case in which a company's primary worth is the IP it controls, an alternative to acquiring full licensing rights is to buy the company. It is hard to separate the true IP value from other company assets. At least two-thirds of the U.S. firm's revenue was derived from the product. No estimate of the companies' other assets was made as part of this study.

Reverse Engineering

Reverse engineering is the process of developing the design and manufacturing capability from a physical copy of the product, but without the assistance of development data or original drawings. This approach would be less costly and faster than the original development previously described. Reverse engineering[1] involves the following steps 1) disassembly; 2) measurement; 3) design recovery; 4) prototype and 5) testing.

The key to estimating the cost is the number of complex parts. Assuming that both the foreign licensee and the U.S. firm use some components from sources requiring no special development, these parts would not be included in the parts list. Excluding off-the-shelf items, the parts count from the bill of materials is about 340. The cost of taking a single part and laser or tool scanning from a reference jig is about $300. The data are then used to produce a CAD/CAM drawing at a cost of $200 each. At $500 per part, for 340 parts, the basic drawing can be reverse engineered for approximately $170,000.

Additional work is required to check the drawings against each other for clearance and manufacturing tolerances that must be estimated for each part. This integration activity would be no more than $100 per part. Clearances are done by computer software and the tolerances by industry standards. Thus, the cost of this portion of reverse engineering would be only $34,000.

Analysis of materials used may require chemical or mass spectrometer sample analysis. Heat treating of materials may be suggested by alloy and hardness measurements. Mass spectrometer analysis per part would cost about $300. Material specification would cost $102,000.

This brings the total cost estimate of reverse engineering to only $306,000.

Even with drawings and specifications in hand, much work is still required to set up a manufacturing system and test of the product. The prototype construction and testing are the most expensive steps in the reverse engineering process. From the R&D cost breakdown provided by the U.S. firm, the cost of prototyping, testing, developing manuals, and maintenance schedules would be at least $40 million. ***This would bring the total cost of reverse engineering***

[1] *Reverse Engineering*, Kathryn A. Ingle, McGraw-Hill, 1994.

Case Study

to about $41 million or about 37% of the original development cost of $112 million. This is consistent with examples described by Ingle.[2]

The degree of reverse engineering or use of the U.S. firm's intellectual property may be estimated by comparing the final products. Comparison data sheets suggest that while general appearance and functional performance are very close look-a-likes, the detail dimensions are all slightly different.

While some features of the U.S. firm's product are reproduced in the foreign competitor's produced product, none of the features were considered patentable by the U.S. firm.

Testing of the product during development by the U.S. firm took 6 years and was an integral part of the product development process. The foreign competitor produced product was developed in less than 3 years and had the advantage of the U.S. firm's operational information. It should be assumed that a U.S.-produced product was available to the foreign competitor for tear-down and inspection as is common practice in this industry.

The availability of the U.S. firm's IP would have helped accelerate the product development and eliminate any need for some reverse engineering steps. The IP contained the following information:

- Engineering drawings, tooling drawings, and process sheets for all components, assemblies, and parts fabricated by the U.S. firm
- Engineering drawings of all components and assemblies and parts purchased by the U.S. firm from vendors.

The second company to produce a similar product in any industry always brings the product to market faster than the innovator. To what degree the IP accelerated the process can only be estimated within the bounds of the 4-year faster development time.

The availability of the IP may have resulted in reducing the time the foreign competitor required to first produce variations of the product for diverse markets. The time to produce the product was very fast. It took the U.S. firm 7 years to develop the original version of the product, while it took the foreign competitor only 3 years to develop their prototype. It is expected that 2 of the 4-year advantage is attributed to the IP theft. That is, without the U.S. firm's IP, the foreign competitor would likely have been able to develop the prototype within a 5-year time frame. Thus we estimate the time to market was accelerated by 2 years as a result of the availability of the IP to the foreign competitor.

Loss of Market

The loss of IP to another company may result in loss of markets and the related profit loss is a measure of IP value. This is a common problem with loss to companies in countries where IP

---

[2] Ibid.

protection is weak. Damage awards in the U.S. are commonly based on actual loss of sales that can be traced to the IP theft.

In this case study, the actual loss of sales has yet to occur. The foreign competitor product is just now entering select foreign markets. As a result, the impacts of the IP theft must be based primarily on projected loss of sales and associated profits. Much of the remainder of this study addresses this approach to estimating the impact of the theft of the U.S. firm's intellectual property.

IP Value Summary

In summary, the value derived from the development cost was $112 million over 7 years. The foreign licensing agreement for a limited market would have netted the U.S. firm up to $47 million over 10 years. Reverse engineering would have cost the foreign competitor about $41 million, mostly for prototype and testing. The U.S. firm's loss of net income from the market loss to the foreign competitor's product are described in the following section and range from $54 million to $81 million.

Market Structure

For this particular case, there are several different markets in which the U.S. firm's product, or an alternative competing product can be sold, as follows:

- U.S. government
- U.S. civilian
- Foreign government
- Foreign civilian.

These are discussed in detail in the following subsections.

U.S. Government Market

The U.S. Government accounts for a large share of sales for the U.S. firm's product to date, with a smaller share being made to government contractors. The U.S. Government market is the safest of all the market segments from foreign competitors, but in 1996, represents less than one-half of the market potential. As discussed below, the other, non-U.S. Government markets could be much more threatened by foreign competition.

U.S. Civilian Market

The U.S. civilian market is made up of bulk sales and individual sales. Roughly 15% of the U.S. firm's commercial sales are believed to be bulk sales. It is expected that a large share of the U.S. firm's domestic civilian sales growth will be in bulk sales. Traditionally, bulk sales are made directly by the company, and the local dealers receive a small commission and future parts sales. Bulk sales require relatively fewer sales representatives than sales to individuals.

Case Study

While the U.S. civilian market is smaller than the foreign government market, it is believed to be safer from foreign competition. Any legal recourse the U.S. firm may be able to take against the foreign competitor would be strongest in the U.S. market. Nevertheless, the foreign competitor is well placed in terms of distribution channels across the United States. Should they enter the U.S. market without legal action from the U.S. firm, the foreign competitor would likely be very successful in making inroads into the U.S. firm's existing and forecasted domestic market share. The largest share would likely come from individual sales. However, the foreign competitor would not likely have a natural advantage in bulk sales. In fact, the U.S. firm will have already established a substantial presence in this market.

Foreign Government Market

The foreign government market is the next largest market, after the U.S. government market, both in terms of sales volume to date and in terms of total expected sales. According to the U.S. firm, foreign government sales generally reach levels comparable with sales to the U.S. government, only lagged by a 10-year period. The foreign government market is relatively easy to tackle compared with foreign civilian sales. There are a limited number of marketing contacts to establish and nurture. However, even within the foreign government market, it is assumed that certain countries would develop their own version of such a product and therefore would be an unlikely market for U.S. sales. Furthermore, these foreign producers would likely compete with the U.S. firm in the global market. This possibility remains an unknown relative to this product.

Due to total sales volume it is assumed that no other potential competitor would spend the necessary resources to produce and market a comparable product without the benefit of a secure government market. This market would provide them with a steady source of sales from which to launch future sales. Therefore, for the purposes of this analysis, it is assumed that the foreign competitor would have developed neither a government nor a civilian version of the product without the initial contract.

Foreign Civilian Market

The foreign civilian market has been and will likely continue to be the most difficult market for the U.S. firm. One reason is because they lack a global distribution network of dealers to market directly to individuals. Foreign civilian sales likely will be based mostly on word of mouth and the reputation. Thus, this market would be the easiest market for a competitor with an established sales network to enter. Conversely, the foreign competitor has a global network of dealers and is positioned to enter the foreign civilian market.

Scenario I: Pre-Bid IP Theft

Base Case

Appendix A is a foldout table that presents the forecasts and impacts for Scenario I. Go to Appendix A., open it up, and refer to this table which is referenced in the text throughout the discussion on Scenario I. Lines 4-16 show the base forecast, 1992-2005. The total in the far right column is the sum of all the columns. Total sales forecast are 137,236 units (15R). Sales

Case Study

prior to 1992 totaled 141,780 units. For domestic and foreign civilian sales the U.S. firm provided annual data from 1992 to the first quarter of 1996. They also provided civilian sales to date, through mid-1996. For government data, they provided total quantities sold from the mid-1980s to the end of the first quarter of 1996. For government data, it was necessary to estimate the share of sales by year for the historical period. Newspaper and other press articles reporting total sales or sales to foreign countries were used in helping to estimate the annual sales for domestic and foreign government sales.

The forecasts for 1996 to 2005 were estimated based on the a variety of information. Line 16 shows the number of units the U.S. firm would need to produce on a daily basis in order to fill any one year's worth of orders, based on the total shown in line 15. According to the U.S. firm, the 1996 production levels averaged 25 units per day, the minimum level of economic production based on the current price of the product. While they expect this number to grow in the future, they said it is unlikely to grow much beyond 50. In our forecast, we peak at 51 units per day in 2000 and 2001. We used the maximum units per day to help determine the maximum total forecast per year.

The wholesale average price for all markets is about $51,000. Special product features for most buyers increases the purchase price by 10% to 15%.

The initial contract forecast (line 7) is based on a total of roughly 10,000 units for the forecast period, 1992-2005, half of the original request for proposal, but more than the 2,000 originally ordered from the foreign competitor. It is assumed that the bulk of the orders would be ordered for delivery between 1994 and 1998, with small, incremental additions for the following years. Note that even though the units related to the lost contract are shown in this table, they are not counted in the yearly totals, nor are they used in the calculations of units per day. They are included to help calculate the royalty loss, which will be discussed later in the report. For the purposes of this base forecast, it is assumed that these units would have been produced by the foreign licensee upon winning the contract.

It is assumed that the bulk of new orders would come from foreign government sales, as shown in "Other Government" in Figure 1. Figure 1 shows the relative share of each major market for total forecast sales, 1992 to 2005.

For the other foreign government forecasts, it was assumed that the U.S. firm would be successful in capturing roughly half of the potential foreign government market. The U.S. firm claims that foreign government sales roughly equal U.S. government sales, only lagged by 10 years. At the end of 1995, U.S. government sales totaled roughly 119,000 units (including sales prior to 1992.)

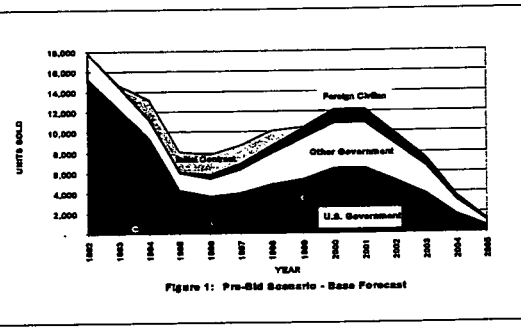

Figure 1: Pre-Bid Scenario - Base Forecast

Case Study

It is estimated that foreign sales would total 56,000 units over the entire period, including sales before 1992, or 46,363 from 1992 to 2005. In this pre-bid scenario, it is assumed for the base case that the foreign licensee does not enter the other foreign markets (government or civilian), because it would compete with the U.S. firm's market. We are also assuming for the base case that the foreign competitor, lacking the incentive of winning the initial contract, has elected to not produce a product that can compete with that of the U.S. firm.

The foreign civilian market is forecast at slightly more than one-third of the level of U.S. civilian sales. The U. S. firm has not made a concentrated effort in targeting the foreign commercial market. Sales in this market are direct sales to individuals placing orders with the U.S. firm. Therefore, it is assumed this market will not be a significant sustaining market for the U.S. firm. For the U.S. government market, we assumed that sales would continue to be flat from 1996 through 1999. Starting in the year 2000, the U.S. firm would likely start seeing reorders for replacement purchases in the mid-1980s. The U.S. civilian market is forecast to reach nearly 22,000 units through 2005.

The domestic civilian market is split into bulk and individual sales by dealers. In 1996, bulk sales totaled roughly 15% of total domestic civilian sales. The U.S. firm is making a significant effort to market directly to the bulk sales market and therefore is expected to increase the share of bulk sales relative to its total domestic civilian sales. For the purposes of our analysis, we assume that bulk sales continues to capture an increasingly larger share of the domestic sales, until it reaches 50% in 2003. Domestic sales overall are expected to increase by slightly more than double overall, to a peak of 3,000 units per year in 1999 through 2001.

For all of the forecasts, we have assumed the value of the design will decline during the last 5 years (2001 to 2005) as various components are replaced by new advances in technology. Sales may continue to prosper, but the product will contain few of the unique design features present in the product at the time of the IP theft. The reduction in IP content is assumed to drop from 100% in 2001 to 10% in 2005.

Property Loss Case

Market Impacts:

In calculating expected future loss of market, it is necessary to make numerous assumptions as to what is likely to happen in the future. We have attempted to make reasonable forecasts, given the information at hand. These forecasts are provided in this section. However, because of the nature of forecasting (and its inherent uncertainty), we have also provided a section (Sensitivity Analysis) that describes the loss estimates given forecasts that are higher and lower in volume and shares than those provided below. The loss estimates will provide an indication of the sensitivity of the model to the forecasts and provide upper and lower bounds for the analysis.

Under the pre-bid scenario, it is assumed that the foreign competitor had access to the U.S. firm's IP before the awarding of the contract. Therefore, the loss to the U.S. firm would include the royalties and the license fee that would have been generated upon the foreign licensee winning

the contract. In addition, the U.S. firm would lose market share and, therefore, sales revenue as a result of the foreign competitor entering other foreign markets.

It is believed that the U.S. Government market will remain free from foreign competition. Therefore, there are three markets in which the impact will be felt:

- The foreign government market
  - initial contract
  - other
- The foreign civilian market
- The U.S. civilian market
  - bulk
  - individual.

Lines 17 through 29 of the table in Appendix A shows the forecast for sales by the U.S. firm under the IP theft case. As expected, the U.S. firm's forecasted sales are lower than in the base forecast. The bottom portion of page 1 of the table in Appendix A (lines 30-42) shows the net forecast, or lost sales, resulting from the theft of the U.S. firm's IP. Below is a summary of each IP theft forecast and the resulting sales lost because of the IP theft.

In the foreign government market, the lost royalties and license fees, which are a direct result of the foreign licensee not winning the "initial contract," are calculated separately from the "other" government market. For the other government market, it is estimated that the foreign competitor's market entry would start to show up in 1997, capturing 10% of the annual foreign government market, and gradually increasing up to a 50% annual market share by the year 2005. This would result in a total loss of sales of approximately $364 million or 7,128 units over the affected period (Table 1).

Table 1. Revenue and Sales Loss from Foreign Government Market

Impact	1992 - 1996	1997 - 2001	2002 - 2005	Total
License fee ($M)	1.0			1.0
Royalties ($M)	12.3	7.4	0.8	20.5
Sales revenue ($M)	0	201.7	161.8	363.5

For the foreign civilian market, the impact would likely be felt more quickly, but the total loss would be less, because the U.S. firm has not made substantial inroads into the foreign civilian market. The foreign competitor would take some of the U.S. firm's market share, but it would also likely generate additional market, based on the foreign competitor's extensive distribution network. It is forecast that the foreign competitor would capture 5% of the U.S. firm's foreign civilian market in 1997, and by 2002, it would have 50% of the U.S. firm's total market, leaving the U.S. firm with about 480 units per year. Even without any concerted effort at marketing overseas, it is assumed that the U.S. firm will continue to hold onto a small share of the foreign

Case Study

market as individuals place orders for the original product. The loss of foreign civilian sales would total roughly 2,440 units, or $124.4 million (Table 2).

Table 2. Revenue Loss from Foreign Civilian Market

Impact	1992 - 1996	1997 - 2001	2002 - 2005	Total
Sales ($ M)	0	69.4	55.1	124.4

The domestic civilian market is split into two parts for the purpose of calculating loss estimates: fleet sales and individual sales. For the purposes of our analysis, we are assuming that the foreign competitor will choose to enter the U.S. civilian market, even though it is not clear that they would in fact choose such an option. Even so, it is likely that the foreign competitor would go after the more accessible markets first; that is, the foreign markets. Starting in 1999, it is projected that the foreign competitor would capture 5% of the U.S. market, working up to 50% by 2004. It is estimated that the foreign competitor would not enter the U.S. bulk market until the year 2000, after it has started to roll out a version for individual sales in the U.S. civilian market. It is estimated that the foreign competitor would capture 10% of the U.S. bulk market in the year 2000 and peak at 33% of the market in 2003. The loss of civilian sales would total an estimated 2,872 units, or $146.5 million (Table 3).

Table 3. Revenue Loss from Domestic Civilian Market

Impact	1992 - 1996	1997 - 2001	2002 - 2005	Total
Bulk	0	14.5	31.2	45.7
Individual	0	42.8	58.0	100.8
Total U.S. Civilian	0	57.4	89.2	146.5

Overall, for all affected markets, the total loss of sales is estimated at almost $634 million, plus an additional $13.3 million loss in revenue from royalties and a license fee. The loss of sales in units is shown in Figure 2.

National Impacts

Description of the Model:

To determine national impacts that might result from lost production, we used a computer model of the economy, based on the 1987 benchmark Input-Output (I/O) table of the United States. This computer model, the Sectoral Energy/

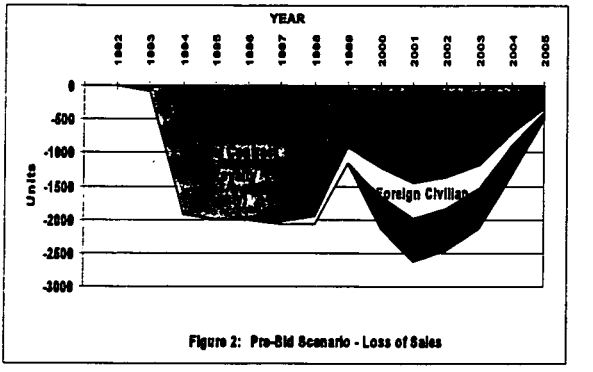

Figure 2: Pre-Bid Scenario - Loss of Sales

Case Study

Employment Analysis and Data System (SEADS-PC), allows the examination of the impact of a loss of sales on energy use and employment for 85 industry sectors of the economy and for the economy as a whole. The model is used here to calculate total employment impacts of the IP theft. A document describing this model, *Methodology, Capabilities, and an Example: Employment Impacts of the Climate Change Action Plan*[3] is included in Appendix B.

Because our sales numbers are in 1996 dollars, the first task was to convert these numbers to the benchmark I/O table year, 1987. The second task was to reduce the output of the comparable industry by the equivalent of $100 million in 1996 dollars. The SEADS-PC model calculates job impacts per $100 million reduction in sales. This calculation proceeded as follows:

- Multiply the capital goods deflator (Economic Report of the President, 1995) for 1995 by the ratio of the deflator for 1995 divided by the deflator for 1994. This suggests a price increase from 1995 to 1996 of about 2% and yields an index of 142.7.
- Divide the index for 1987 (111.7) by this number to convert 1996 dollars into 1987 dollars. Thus $100 million in 1996 is the same as $78.2 million in 1987.
- Reduce final demand for the product by $78.2 million and compare the employment impact of this reduction to the base case of no change. The following results were obtained. The major industries affected by the reduction, as would be expected, are the comparable industry, wholesale and retail trade, primary metals, stampings, and rubber and plastics.

SEADS-PC provides details on both hours and jobs, with somewhat greater resolution on hours than jobs. The table on the right gives hours, reported in thousands, and jobs, calculated based on 1,880 hours per job-year. Note that the $100 million reduction in orders for the comparable industry translates into 452 jobs. Thus a $1 million reduction in parts supplied to the U.S. firm translates into a loss of 4.52 jobs to the suppliers.

Employment Impacts of a $100 Million Reduction in Sales

Industry	Jobs	Hours (1,000s)
Rubber & Plastics	48	89.5
Primary Metals	48	91.0
Stampings	44	83.3
Comparable Industry	452	850.1
Trade	210	394.6
All Other	586	1,100.9
TOTAL	1,388	2,609.4

For the economy as a whole, the equivalent of a $100 million loss of sales is about 1,388 jobs, or 2.6 million hours of lost work. Since the aggregate impact of lost sales is about $900 million, the employment impacts would be nine times those reported in the table, or 12,500 jobs.

[3] J.M. Roop, D.M. Anderson, and R.W. Schultz. September 1995. *Methodology, Capabilities, and an Example: Employment Impacts of the Climate Change Action Plan.* PNL-10760, Pacific Northwest National Laboratory, Richland, Washington. The model was developed for the Policy Office of the U.S. Department of Energy. The point of contact is Peggy Pokolate, (202) 586-6430.

Case Study

Application of the Model to the Case:

The second half of the table in Appendix A presents the impacts of the IP theft to the nation, the company and suppliers, (lines 44-72). Lines 44 through 53 show national impacts. The national impacts of the foreign competitor having access to the U.S. firm's intellectual property will be manifested in loss of trade and royalties revenues, impacts on direct and indirect jobs, and corporate and payroll taxes.

Trade Impacts: Trade impacts (line 46) in dollar terms are calculated by taking the net change in foreign exports (foreign export minus the initial contract shown in lines 31-33) plus imports (shown as civilian losses in line 38) times the average unit price of $51,000 plus 12.5% for extra add-on equipment.[4] The total dollar trade impact totals $714 million through 2005.

Royalty Impacts: Loss of royalties (line 47) due to the loss of contract sales by the foreign licensee are calculated as follows. Starting in 1994, when it is assumed the foreign licensee would have started producing had they won the contract, the royalty loss is calculated as:

*lost sales (1,915 in 1994) * unit sales price of $51,000 * 4% royalty ~ $4 million*

Lost royalties range from a high of $4 million (1994 through 1997) to less than $1 million (from 1999 through 2005). The reason for such low numbers is the estimated small size of the foreign government market -- a high of 2,000 units sold in 1995 and 1996 to 100 units by 1999. The $1 million in the 1992 royalty column comes from the "up-front" license fee paid by the foreign licensee to the U.S. firm.

Job Impacts: Job impacts (line 50) from the U.S. firm's loss of IP at the national level can be broken into three categories. Total jobs are the sum of company, supplier, and indirect jobs (lines 51-53).[5] Again, these are the total jobs lost because the U.S. firm lost its IP to the foreign competitor and the resulting market infringements produced by such a loss. Figure 3 shows the jobs lost due to the IP theft.

Selected years showing jobs lost in terms of job-year equivalents is as follows:

1997	2001	2005	Total
309	1,800	284	9,452

[4] Remember that the unit sales by the foreign licensee are included in the base case and not the property loss case because the market has now been taken over by the foreign competitor. The loss in initial contract sales from the base case would manifest itself in the royalty loss (line 47).

[5] Company jobs are those directly associated with production of the product at the company. Supplier jobs are those jobs directly associated with supplying parts to the company. Indirect jobs are defined as additional jobs created by the employment associated with the U.S. firm's suppliers.

Case Study

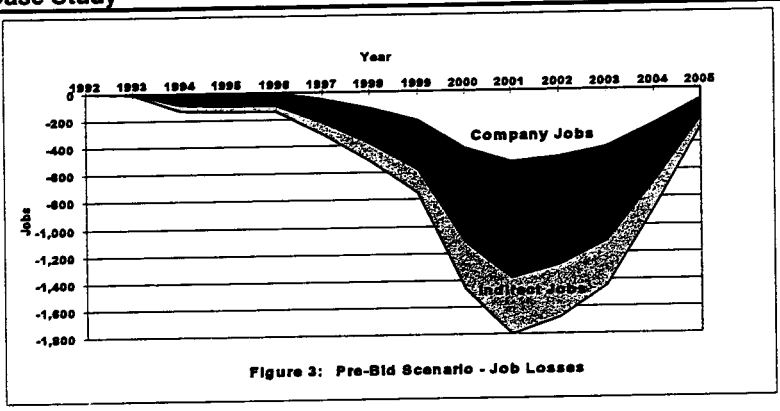

Figure 3: Pre-Bid Scenario - Job Losses

Tax Impacts: Payroll loss (line 48) is based on total jobs lost and is figured as follows. Annual before tax earnings per employee is estimated at $40,000 a year. Federal payroll taxes[6] are approximately 15% and result in $2 million in lost payroll taxes in 1997. Lost payroll taxes jump to $5 million in 1999, almost double to $9 million in the year 2000.

National corporate taxes (line 49) lost are composed of the total company corporate and supplier corporate taxes lost. Corporate tax losses peak at $13 million in 2001 and total $72 million through 2005. This is the sum of lines 62 and 70.

Company Impacts

The loss of sales to the foreign competitor translates into company impacts to the U.S. firm through losses in dollar revenue, profits, and royalties. Remember that the lost sales to the foreign licensee are reflected in lost royalty revenue. Because of lower profits, taxes will decrease, partially offsetting some of the losses. Figure 4 shows these losses and gains. Company impacts are shown in Appendix A (lines 55-63.)

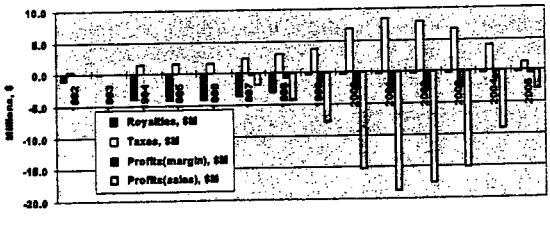

Figure 4: Pre-Bid Scenario - Income loss, $M

6 Defined as social security and Medicare contributions for both the employer and employee.

Case Study

Total Revenue:

The loss in total revenue (line 57) to the U.S. firm reflects the foreign competitor's impact of market infringement on the U.S. firm's foreign government (other) and civilian markets, plus domestic infringement beginning in 1999 on individual sales and in 2000 on bulk sales.

Total revenue lost, which begins in 1997, is calculated the same way as the total national revenue lost (without the 12.5% escalation factor for suppliers add-on equipment, which the U.S. firm does not see in its total revenues):

1997	2001	2005	Total
$13 million	$129 million	$20 million	$634 million

Royalties:

Royalty revenues (line 59) lost are calculated the same as national impacts and are the same as the national royalty revenues as they accrue directly to the company and to no other entity.

Profits:

Company profits from sales (line 60) are first impacted in 1993 by the loss of IP to the foreign competitor. The profit loss is determined by multiplying the total units of lost sales (line 41) minus government sales as a result of the initial contract (line 33), by the profit estimated by the U.S. firm for each unit of production above 25 units per day ($7,478).

The timeline for lost sales profits is as follows:

1997	2001	2005	Total
$2 million	$19 million	$3 million	$93 million

As the foreign competitor begins to compete with the U.S. firm -- 1997 in the foreign markets and 1999/2000 in the domestic market -- one would expect the U.S. firm's profit margins to begin to erode as the competition puts pressure on the U.S. firm's unit price. The effect on profit margins can manifest itself in two ways: one, by not allowing the U.S. firm to raise unit prices to cover the increased manufacturing costs caused by inflation and other factors, or, two, by putting direct pressure on the U.S. firm's unit price, forcing a lower price in order to maintain market share.

Eroding profit margins (line 61) do not begin to show up on the U.S. firm's bottom line until 1997 when the foreign competitor begins impacting foreign government sales. The decrease is $0.3 million[7] and is calculated as follows:

*U.S. civilian and foreign sales * $2,000 profit per unit * (unit sales loss/unit sales made)*

[7] The $0.3 million shows up as a zero in the table in Appendix A due to rounding.

Case Study

When sales losses equal sales made, the foreign competitor would have a 50% market share and the full $2,000 per unit profit loss is applied. When losses are small in the early years, the profit losses are very small.

The timeline for declining profit margin is as follows:

1997	2001	2005	Total
$0.3 million	$3 million	$0.4 million	$16 million

This brings the total profit loss to the U.S. firm to $109 million.

Taxes:

Reduced company corporate taxes (line 62) are calculated by adding the U.S. firm's lost profits and royalties together and multiplying that by a marginal corporate income tax rate of 38%. The 38% consists of 35% for federal tax and 3% for the state tax. The timeline is as follows:

1997	2001	2005	Total
$2 million	$8 million	$1 million	$50 million

Net income loss (line 58) is the sum of royalties and profit losses, plus the reduction in taxes paid by the company as a result of the losses (sum of lines 59-62). Net income loss through 2005 totals $81 million.

Jobs:

The loss in company revenue impacts the number of employees working at the U.S. firm, as the company sees a decline in the number of units manufactured and the revenue received. Lost company jobs (line 63) are estimated by multiplying the number of lost units manufactured per day (units in 1997) by 49, which represents the number of direct and indirect jobs necessary to produce one unit per day.

The timeline for company jobs lost in terms of job-year equivalents is as follows:

1997	2001	2005	Total
54	527	82	2,600

Supplier Impacts

Revenues:

Supplier impacts are shown in Appendix A (lines 66-72). As the U.S. firm's market share erodes, the revenue to the U.S. firm's suppliers will begin eroding as well. The supplier revenue loss (line 68) of $18 million in 1997 is calculated as follows. The 1997 revenue loss by the U.S. firm ($13 million) is multiplied by the ratio of that portion of the unit price of $51,408 that accrues to the supplier (or $30,280) plus the 12.5% of the unit price that represents aftermarket vendor/supplier

Case Study

add-ons, which the U.S. firm does not receive but the supplier does, plus foregone sales to the initial contract foreign market of $5,000 per unit. The timeline for the lost revenues is as follows:

1997	2000	2005	Total
$18 million	$92 million	$15 million	$503 million

Profits:

Supplier profits (line 69) are not impacted until 1997 when the foreign competitor's encroachment on some of the U.S. firm's foreign sales market begins. The lost supplier profits are calculated by multiplying the supplier revenue by a 12.5% supplier profit rate.

Taxes (line 70) not paid by the suppliers are calculated by multiplying the suppliers' lost profits by the marginal tax rate of 35%. Foregone taxes are about $1 million until 1998, after which they exceed $2 million. The foregone tax revenue loss totals $22 million through 2005.

Jobs:

Lost supplier jobs in terms of job-year equivalents (line 71) are calculated by multiplying the supplier's lost revenues by a factor of 4.52, which is the number of jobs supported by each $1 million of supplier revenue:

1997	2001	2005	Total
83	417	66	2,274

Also, 9.28 indirect jobs (or second-tier supplier jobs, shown on line 72) are lost by each $1 million decline in total supplier revenue (as discussed in section called "Description of Model.") Hence, the indirect jobs lost in 1997 are calculated by taking the 4.52 factor times total supplier revenue lost, or $16 million, which results in an estimated 171 jobs lost in 1997. The number peaks at 856 in 2001.

Scenario II: Post-Bid IP Theft

Base Case

The table presented in Appendix A will no longer be required. The Table in Appendix C is a fold out which shows Scenario II, the post-bid IP theft case. Go to Appendix C, open it up and refer to this table which will be referenced throughout this section.

Under the post-bid scenario, it is assumed that the transfer of IP took place after the foreign competitor won the contract. Therefore, the U.S. firm's foreign licensee would not have sold any units under the base case and the U.S. firm would not earn royalties or additional license fees. However, as a result of having access to the U.S. firm's IP, the foreign competitor would be able to enter the market approximately 2 years sooner than it would have been able to do had it not had that access.

Case Study

The first section of the table in Appendix C (lines 4-16) shows the base case for the post-bid scenario. The same formulas were applied to this base case as in the pre-bid property theft case, only delayed by 2 years. For example, it is assumed under this base case scenario that the foreign competitor would gain 10% of the other foreign market in 1999, even though they do not have access to the U.S. firm's IP. With the help of the U.S. firm's IP, under the post-bid theft case, it is assumed that they would enter the market in 1997.

Property Theft Case

Under the post-bid scenario, the property theft case will be the same as under the pre-bid scenario. The impact will be the 2-year advantage the foreign competitor gains in entering the market. That is, the property theft case minus the pre-bid scenario will give us the net loss to the U.S. firm. Lines 17-72 of the table shows the post-bid IP theft impacts on the market, the nation, the company, and the suppliers.

Market Impact:

The post-bid IP theft would result in the sales loss of roughly 11,493 units (worth about $586 million), as shown in Figure 5. Foreign government sales (not including the initial contract) would account for about 50% of these lost sales. The remaining losses are roughly split between domestic and foreign civilian sales. The net sales loss under this scenario is roughly one-half the 22,441 lost sales experienced under the scenario I (Pre-Bid IP Theft).

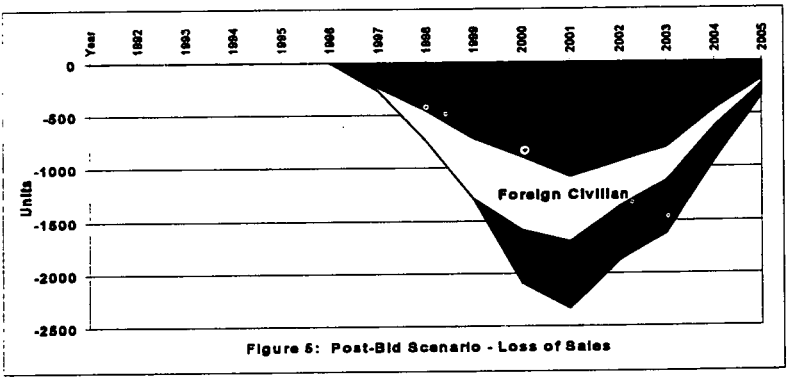

Figure 5: Post-Bid Scenario - Loss of Sales

National Impact:

At $659 million, the trade impacts (line 46) under this scenario are roughly 92% of the level of those under the first scenario. Since it is likely that the foreign competitor will enter the foreign market before the U.S. market, it makes sense that the largest impacts will take place against the U.S. firm's foreign sales. As mentioned above, there are no royalty impacts, because it is

Case Study

assumed that the foreign competitor won the initial contract without the aid of the U.S. firm's IP. The average annual loss of jobs under this scenario is roughly 86% of that under the first scenario. Figure 6 shows the total job losses under this scenario. Below are job losses at the national, company, supplier, and indirect levels (lines 50-53):

	1997	2001	2005
National	185	1,661	234
Company	54	488	69
Supplier	43	384	54
Indirect	88	789	111

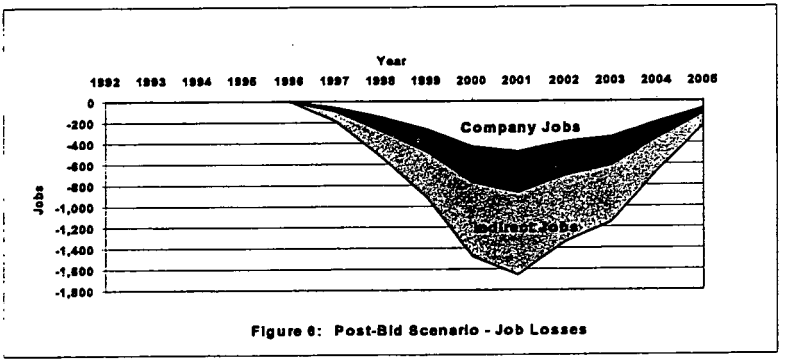

Figure 6: Post-Bid Scenario - Job Losses

At $105 million, the loss of federal revenue from corporate and payroll taxes (lines 48 and 49) for this scenario compares with $129 million under the first scenario.

Through 2005, losses in company net income (line 58) totaled $62 million compared with $81 million in the first scenario. Profit losses totaled $100 million under this scenario. Figure 7 shows profit losses incurred under this scenario.

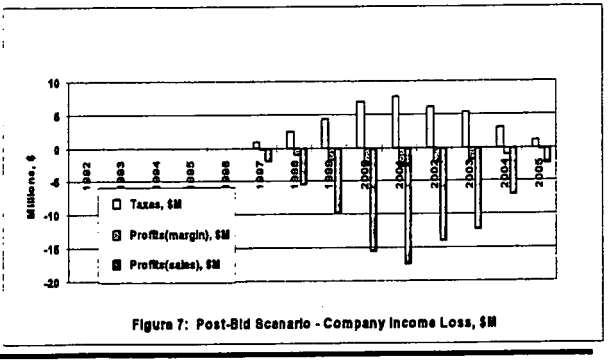

Figure 7: Post-Bid Scenario - Company Income Loss, $M

Suppliers' Impacts:

Suppliers' lost revenues (line 68) total $419 million through 2005, 83% of that in the first

scenario. Losses to suppliers' profits total $52 million under this scenario, compared with $63 million under the first scenario.

Sensitivity Analysis

The forecasts in this case study are at best estimates of what could happen, given a certain scenario. In order to get a sense of how different forecasts might affect the results, we have simulated the model using low and high forecasts, in addition to the "moderate" level forecasts used in the analysis above. The number of units sold for the low, moderate, and high forecasts are shown in Table 4, with market share loss percentage in parenthesis. This analysis is only done for the Pre-bid IP theft scenario.

Table 4. Low, Moderate, and High Unit Sales Forecasts for Sensitivity Analysis

Market Segment	Low	Moderate (from scenarios)	High
Foreign: initial contract	2,000	10,000	20,000
Foreign: Other government loss	4,435 (25%)	7,128 (50%)	10,448 (75%)
Foreign civilian loss	1,220 (25%)	2,440 (50%)	3,890 (75%)
U.S. civilian loss	972 (25%)	2,873 (50%)	4,199 (75%)

Profits

The results of this forecast are shown in Table 5. Loss of net income as a measure of damages from IP theft are sensitive to forecasts of market shares. The best measure of total economic damage to the U.S. firm is the sum of their profit and royalty losses, less taxes, throughout the product life. This measure, called the net income, totals the annual loss from initial market penetration through 2005. In the base forecast (moderate), the market share credited to the foreign competitor was 50% by 2005. The sensitivity analysis examines the impact of 25% and 75% shares. Shares do not apply to the initial foreign contract, as it would be all (100%) either the foreign competitor's or the foreign licensee's. The range for the initial foreign contract

Table 5. U.S. Firm Profit and Royalty Loss for Low, Moderate, and High Forecasts, in $M

Market Segment	Low	Moderate (from scenarios)	High
Foreign: initial contract	71	81	93
Foreign: other government loss	66	81	93
Foreign civilian loss	74	81	89
U.S. civilian loss	71	81	88

market comes from the information provided by the foreign licensee on the expected market size at the time of their bid and their indication that initial orders from the government have been very small. For the U.S. civilian low market case, the 25% refers to the individual market, while the bulk sales market loss was set to zero. The U.S. firm net income losses range from $66 million to $93 million as a result of the sensitivity calculations.

Jobs:

The effect of the sensitivity runs on jobs are shown in Table 6. The employment units are person-years and mainly occur during the last 10 years of the product life cycle (1995 - 2005). The changes from each of the market segments are additive, so combination of sensitivity can easily be estimated.

Table 6. National Employment (person-years) Loss for Low, Moderate, and High Forecasts

Market Segment	Low	Moderate (from scenarios)	High
Foreign: initial contract	8,990	9,542	10,232
Foreign: Other government loss	7,626	9,542	11,904
Foreign civilian loss	8,674	9,542	10,574
U.S. civilian loss	8,189	9,542	10,485

Results:

Overall, these results suggest that the first scenario findings of IP losses are not very sensitive to these dramatic changes in market share captured by the foreign competitor. If the foreign competitor captures only 25% of the markets shown in Table 4, net income would only improve by about 12%. If they capture 75% of the market, net income would be worse by only 14%. And the sensitivity is similar for jobs. A lower foreign competitor market share would only improve jobs by 12% and a higher share would reduce jobs by 13%.

IV - Applicability of Methodology to Other Cases

The methodology that was developed in this paper and applied in the previous section to a specific case was intended to be a generic framework that could be applied to any case. The purpose of this section is to quickly review a different case study provided by the Federal Bureau of Investigation to determine if and how the generic framework could be used under a different example.

Ssangyong Group, a Korean company, was accused by Litton Systems, Inc., of the theft of IP related to radar and electronic countermeasures (ECM) used in war planes. This section will briefly provide background to this case, discuss how the methodology described in this report might be used to estimate impacts of the loss of that IP, then explain the outcome of the litigation brought by Litton.

Background

In early 1989 Ssangyong, a Korean manufacturer of microwave tubes, power supplies, and amplifiers, invested $1.5 million in M-Square Microtek, Inc., a California microwave technology company that had access to Klystrons (used in ground radar), Helix Traveling Wave Tube (TWT, used in jamming and radar), Coupled Cavity TWT (used in radar and fire control), and the power supplies for all tubes. These technologies, developed by Litton, are used in advanced military war planes as part of their ECM equipment and are subject to Defense Department export controls. In addition to the purchase price, Ssangyong infused the company with $17 million. In November 1989, Litton Systems filed suit, alleging theft of drawings of the indicated technologies. M-Square has subsequently gone bankrupt and Ssangyong and Goldstar, a Korean manufacturer of radar and jammers, have embarked on a joint venture.

Applying the Methodology

Litton requested that the Courts judge that Ssangyong pay Litton either the license value or the research costs Ssangyong saved through the theft of this property. (Before the suit, Litton made a settlement offer of $2 million.) In a proffer to the court, Litton's attorneys outlined some relevant considerations, that allow a superficial estimation of impacts. These are adequate and illustrative for this study.

While adequate, they fall far short of allowing an application of the methodology directly. The proffer to the court is designed to rebut the interpretations and assertions of Ssangyong to the court, and do not contain the detailed data necessary to apply the methodology directly. Nonetheless, in attempting to establish damages to Litton, the proffer does appeal to economic and financial data that the method would require.

The military technology could have limited commercial applications, so the worldwide market was estimated by Ssangyong at $2 billion, with sales of $120 million per year. This compares with Litton sales of $60-100 million per year. Litton could not have captured these foreign sales as long as the technology was banned for export. To the extent that Goldstar marketed these technologies (in commercial markets) within the United States, they might have cut into Litton

sales. There is no estimate of this impact in the proffer, suggesting that Litton did not consider this a serious challenge to its domestic market. At some time in the future, Litton would have had a commercial advantage in world markets after the Defense Department ban on exports was lifted. Historic evidence could be marshalled to determine the likely pattern of export controls being lifted after new technologies substitute for critical military applications.

The estimate of the cost of developing this technology was $88 million. For a world market of $2 billion, it seems reasonable that someone, possibly Goldstar, would have undertaken the R&D necessary to develop a competitive technology, so as with the in-depth analysis of the previous case, the impact would be, in large measure, a question of timing. With the lifting of the export ban, Litton would be expected to participate in military and commercial sales outside the United States. If Goldstar had captured part of the market as a result of the theft, these would be counted as part of the loss to Litton.

Adjudicated Results

The court action took nearly six years to resolve. Legal fees came to $7 million for Ssangyong and $3.5 million for Litton. The court found in Litton's favor and Ssangyong had to pay Litton $65 million in punitive damages, in addition to picking up Litton's legal fees. Including the investments in M-Square, Ssangyong lost a total of $94.5 million, considerably more than it would have cost to develop the technology and over $90 million more than Litton was willing to settle for before going to trial.

Applicability

While the examination of this case does not qualify as a full case study, we believe that the framework described in chapter II would generally apply. A more extensive analysis would be required to fully test the framework against this case.

V - Lessons Learned and Recommendations

Lessons Learned about the Case and Recommendations for U.S. Business

- The case study dealt with a complex piece of equipment. We learned that design is a very important part of the value of a product, but is not effectively protected from IP theft. Even though the foreign competitor did not copy many of the individual components of the U.S. product, it appears that it did copy the overall design. ***It may be in the interest of public policy to strengthen U.S. laws to protect designs from exploitation.***

- ***U.S. companies should not assume that foreign governments will give U.S. proprietary information the same level of protection as that provided by the U.S. Government.***

- The U.S. firm entered into a licensee agreement with a foreign company for a technology whose IP could not effectively be protected, incurring losses as a result of theft of their IP. Had the product embodied technology that was expected to rapidly evolve beyond the IP shared with their licensee, the U.S. firm would have effectively protected their own IP through innovation. Unfortunately, this technology was not expected to change significantly for at least a decade. ***U.S. companies might consider whether it is worth the risk to share their IP with foreign companies if this IP is expected to have a long product life cycle and cannot be effectively protected.***

- In a show of good faith, the U.S. firm shared their IP with a foreign company prior to finalizing a license agreement. It is not clear that they were injured by this act, but ***U.S. companies should be careful how and with whom they share their IP.***

- The initial foreign contract request for proposal called for 20,000 units, but the actual number of unit sales awarded to the contract winner, was only 2,000. It is unlikely that the U.S. firm would have entered into the license arrangement had they been aware that sales would have been only 2,000 units. ***This raises the question whether a U.S. manufacturer was baited into entering the contract bid through an inflated request for proposal issued by the foreign government.***

Lessons Learned and Recommendations for Future Studies

- A major lesson learned is the role the company plays in obtaining data. The U.S. firm's cooperation in this case was critical to reach a logical, objective treatment of the case. They provided data and reviewed our forecasts to see if they were reasonable. ***Cooperation of the alleged injured party in sharing data and information is critical.***

Case Study

- It would have been of help to learn which markets the foreign competitor was trying to enter, and what they saw as a reasonable goal for market share. It also would have been helpful to have the foreign government documents pertaining to the original solicitation, as well as the final contract awarded. This information likely would have obviated the need for two separate scenarios in this case study. ***Collateral data provided by the FBI can make a difference on the number of assumptions made during the analysis.***

- There are several ways to value IP, including assessing the development cost, potential revenue through licensing arrangements, reverse engineering and market analysis. In this case study, we found that ***market analysis was the most effective method for evaluating the impact of IP theft.***

Appendices

Appendix A
Pre-Bid Scenario Table

Case Study

Pre-Bid Scenario Table

	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
2	Product sales, units		1995 unit value:		$31,000			Royalty:	4%		1.0	0.8	0.6	0.3	0.1	
3	Year	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	Total
4	Base forecast															
5	Foreign - Total	2,510	2,335	3,616	3,826	4,193	4,700	5,800	6,100	5,800	5,800	4,680	3,620	1,810	670	64,010
6	Government	2,500	2,285	3,715	3,700	3,763	4,100	4,500	4,100	4,600	4,600	3,700	2,800	1,450	550	46,363
7	Initial Contract		85	1,915	2,000	2,000	1,800	1,500	100	100	100	100	100	100	100	10,000
8	Other Government	2,500	2,200	1,800	1,700	1,763	2,300	3,000	4,000	4,500	4,500	3,600	2,700	1,350	450	36,363
9	Foreign Civilian	10	50	101	126	400	600	800	1,000	1,200	1,200	980	720	360	120	7,847
10	Domestic - Total	15,303	12,350	9,400	4,240	3,613	4,000	4,650	5,350	5,400	5,400	5,120	3,840	1,770	670	83,228
11	U.S. Government	15,000	12,000	9,000	3,000	2,350	2,350	2,350	2,350	3,400	3,400	2,720	2,040	1,020	340	61,320
12	Civilian	303	350	400	1,240	1,263	1,650	2,500	3,000	3,000	3,000	2,400	1,800	750	250	21,906
13	Individual	303	333	360	1,054	1,074	1,320	1,875	2,100	1,950	1,800	1,320	900	375	125	14,888
14	Bulk	-	18	40	186	189	330	625	900	1,050	1,200	1,080	900	375	125	7,018
15	Total	17,813	14,685	13,216	8,066	7,776	8,700	10,150	10,450	12,200	12,200	9,780	7,360	3,580	1,260	137,236
16	U.S. units/day	76	62	48	26	25	29	37	44	51	51	41	31	15	5	
17	Property loss forecast															
18	Foreign	2,510	2,250	1,801	1,626	2,193	2,640	3,250	3,950	4,135	3,810	2,820	1,980	923	285	94,443
19	Government	2,500	2,200	1,800	1,700	1,763	2,070	2,550	3,200	3,375	3,150	2,340	1,620	743	225	29,236
20	Initial Contract															-
21	Other Government	2,500	2,200	1,800	1,700	1,763	2,070	2,550	3,200	3,375	3,150	2,340	1,620	743	225	29,236
22	Foreign Civilian	10	50	101	126	400	570	680	750	760	660	480	360	180	60	5,207
23	Domestic - Total	15,303	12,350	9,400	4,240	3,613	4,000	4,650	5,350	5,905	5,770	4,608	3,255	1,324	485	80,353
24	U.S. Government	15,000	12,000	9,000	3,000	2,350	2,350	2,350	2,350	3,400	3,400	2,720	2,040	1,020	340	61,320
25	Civilian	303	350	400	1,240	1,263	1,650	2,500	3,000	2,505	2,370	1,788	1,215	304	145	19,033
26	Individual	303	333	360	1,054	1,074	1,320	1,875	2,100	1,950	1,350	924	540	55	63	12,911
27	Bulk	-	18	40	186	189	330	625	900	945	1,020	864	675	248	83	8,122
28	Total	17,813	14,600	11,301	6,066	5,776	6,640	8,080	9,300	10,080	9,880	7,328	5,235	2,248	770	114,796
29	U.S. units/day	76	62	48	26	25	28	34	40	43	41	31	22	10	3	
30	Net forecast															
31	Foreign	0	-85	-1,915	-2,000	-2,000	-2,060	-2,070	-1,150	-1,845	-1,990	-1,840	-1,640	-888	-385	-19,888
32	Government	0	-85	-1,915	-2,000	-2,000	-2,030	-1,950	-900	-1,225	-1,450	-1,360	-1,180	-708	-325	-17,128
33	Initial Contract	0	-85	-1,915	-2,000	-2,000	-1,800	-1,500	-100	-100	-100	-100	-100	-100	-100	-10,000
34	Other Government	0	0	0	0	0	-230	-450	-800	-1,125	-1,350	-1,260	-1,080	-608	-225	-7,128
35	Foreign Civilian	0	0	0	0	0	-30	-120	-250	-420	-540	-480	-360	-180	-60	-2,440
36	Domestic - Total	0	0	0	0	0	0	0	0	-495	-630	-612	-585	-446	-105	-2,873
37	U.S. Government	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
38	Civilian	0	0	0	0	0	0	0	0	-495	-630	-612	-585	-446	-105	-2,873
39	Individual	0	0	0	0	0	0	0	0	-390	-450	-396	-360	-319	-83	-1,977
40	Bulk	0	0	0	0	0	0	0	0	-105	-180	-215	-225	-128	-43	-895
41	Total	0	-85	-1,915	-2,000	-2,000	-2,060	-2,070	-1,150	-2,140	-2,620	-2,452	-2,125	-1,334	-490	-22,441
42	U.S.units/day	0	0	0	0	0	-1	-2	-4	-9	-11	-10	-9	-5	-2	
43																
44	National Impacts															
45	Year	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	Total
46	Trade balance, $M	0	0	0	0	0	-15	-33	-50	-117	-145	-135	-118	-71	-22	-714
47	Royalties, $M	-1	0	-4	-4	-4	-4	-3	0	0	0	0	0	0	0	-21
48	Taxes(payroll), $M	0	0	-1	-1	-1	-2	-3	-5	-9	-11	-10	-9	-5	-2	-57
49	Taxes(corp), $M	0	0	-2	-2	-2	-3	-4	-5	-10	-13	-12	-10	-6	-2	-72
50	Total jobs	0	-6	-132	-138	-138	-309	-509	-754	-1,458	-1,800	-1,680	-1,448	-885	-284	-8,542
51	Company jobs	0	0	0	0	0	-54	-119	-219	-426	-527	-492	-423	-258	-82	-2,600
52	Supplier jobs	0	-2	-43	-45	-45	-83	-128	-175	-338	-417	-389	-338	-205	-66	-2,274
53	Indirect jobs	0	-4	-89	-93	-93	-171	-262	-359	-694	-856	-799	-689	-422	-136	-4,668
54																
55	Company Impacts															
56	Year	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	Total
57	Revenue, $M	0	0	0	0	0	-13	-29	-54	-104	-129	-120	-103	-63	-20	-634
58	Net Income	-1	0	-2	-3	-3	-4	-5	-6	-11	-14	-13	-11	-7	-2	-81
59	Royalties, $M	-1.0	-0.2	-3.9	-4.1	-4.1	-3.7	-3.1	-0.2	-0.2	-0.2	-0.2	-0.2	-0.2	-0.2	-21.4
60	Profits(sales), $M	0	0	0	0	0	-2	-4	-8	-15	-18	-18	-15	-9	-3	-93
61	Profits(margin), $M	0	0	0	0	0	0	-1	-2	-3	-3	-3	-2	-1	0	-16
62	Taxes $M	0	0	1	2	2	2	3	4	7	8	8	7	4	1	50
63	Company jobs	0	0	0	0	0	-54	-119	-219	-426	-527	-492	-423	-258	-82	-2,600
64																
65																
66	Supplier Impacts															
67	Year	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	Total
68	Revenue, $M	0	0	-10	-10	-10	-18	-26	-39	-75	-92	-86	-74	-45	-15	-503
69	Profits(sales), $M	0	0	-1	-1	-1	-2	-4	-5	-9	-12	-11	-9	-6	-2	-83
70	Taxes $M	0	0	0	0	0	1	1	2	3	4	4	3	2	1	22
71	Supplier jobs	0	-2	-43	-45	-45	-83	-128	-175	-338	-417	-389	-338	-205	-66	-2,274
72	Indirect jobs	0	-4	-89	-93	-93	-171	-262	-359	-694	-856	-799	-689	-422	-136	-4,668

Case Study

Table Notes:

Note: Because of rounding, figures may not add to the totals shown.
Total column (R): This is the sum of 1992 through 2005.

Base Forecast (lines 4-16): This section presents the original forecast (in units), given no loss of IP.

Initial Contract (line 7): Figures for initial contract represent the expected market under the initial contract. They are included to calculate royalty losses. These figures for the initial contract are not included in the total (line 15) or in the calculation for U.S. units/day.

Total (line 15): Sum of foreign (line 5) and domestic (line 10) sales for any given year. Totals for 1992 - 1996 are based on actual sales. Totals for 1997 - 2005 are forecasted sales.

U.S. units/day (line 16): This is the number of units produced daily in order to fill any one year's worth of orders (line 15.) U.S. units per day is calculated using a one-shift, 235-day work year.

IP Theft Forecast (lines 17-29): This section presents the revised forecast, given a theft of IP.

Net Forecast (lines 30-42): Net losses resulting from the loss of IP. It is calculated by subtracting the property loss forecast from the base forecast.

National Impacts (lines 44-53): This section presents the impacts of the IP theft affecting the nation as a whole.

Trade (line 46): The net trade balance will decrease because of a reduction in U.S. exports, plus an increase in U.S. imports resulting from the IP theft. The reduction in exports is calculated by taking the net change in foreign sales (line 31) minus the initial contract sales. (line 33). The increase in imports is shown as civilian losses in line 38.

Royalties (line 47): The loss in royalties as a result of the foreign licensee not winning the contract. Note that the loss in D55 ($1 million) represents the loss of a license fee that would have been awarded to the U.S. firm had the licensee won the contract. Profit from parts sales tied to the licensing agreement are also included.

Taxes (payroll) (line 48): The loss of payroll taxes resulting from fewer employees earning wages to pay taxes.

Taxes (corporate) (line 49): The loss of corporate income tax resulting from the company and its suppliers earning less revenue and less profits.

Total jobs (line 50): The number of jobs lost throughout the United States as a result of IP theft. This job total includes company, supplier, and indirect jobs. Jobs are represented in person years.

Company jobs (51): The number of jobs lost by the company as a result of IP theft. Jobs are represented in person years.

Supplier jobs (line 52): The number of jobs lost by the company's suppliers as a result of IP theft. Represented in person years.

Indirect jobs (line 53): The loss of indirect jobs lost as a result of jobs lost by the U.S. firm's suppliers.

Company Impacts (lines 55-63): This section presents the financial impacts of IP theft affecting the company.

Revenue (line 57): The loss of company revenue resulting from reduced sales because of the IP theft.

Royalties (line 59): The loss in royalties as a result of the foreign licensee not winning the contract. Note that the loss in D55 ($1 million) represents the loss of a license fee that would have been awarded to the U.S. firm had the foreign licensee won the contract.

Profits (sales) (line 60): The profits resulting from sales are calculated by multiplying the total number of lost sales (line 41) by the standard profit made on each unit ($7.478).

Profits (margin) (line 61): A loss in profits due to a squeeze on the company's profit margin due to increased competition. Margins are squeezed through lower sales prices, and/or through higher per unit costs as the number of units produced per day declines.

Taxes (line 62): The company's taxes will actually decrease as a result of reduced revenues and profits. This is represented as a gain to the company, which partly offsets the loss in profits.

Supplier Impacts (lines 66-72): This section presents the financial impacts affecting the company's suppliers.

Revenue (line 68): The loss of suppliers' revenue resulting from reduced sales because of the IP theft.

Profits (line 69): The loss of profits resulting from a loss of sales. Calculated by multiplying supplier revenue by a 12.5% average supplier profit rate.

Taxes (line 70): The suppliers' taxes will actually decrease as a result of reduced revenues and profits. This is represented as a gain to the suppliers, which partly offsets the losses in profits.

Appendix B

Methodology, Capabilities, and an Example: Employment Impacts of the Climate Change Action Plan

PNL-10760
UC-98F

SEADS:-PC:
Sectoral Energy/Employment
Analysis and Data System

Methodology, Capabilities, and an Example: Employment Impacts of the Climate Change Action Plan

J. M. Roop
D. M. Anderson
R. W. Schultz

September 1995

Prepared for
U.S. Department of Energy
under Contract DE-AC06-76RLO 1830

Pacific Northwest Laboratory
Richland, Washington 99352

Battelle

PNL-10760

PACIFIC NORTHWEST LABORATORY
operated by
BATTELLE MEMORIAL INSTITUTE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC06-76RLO 1830

PNL-10760
UC-98F

SEADS-PC:
Sectoral Energy/Employment
Analysis and Data System

Methodology, Capabilities, and an Example: Employment Impacts of the Climate Change Action Plan

J. M. Roop
D. M. Anderson
R. W. Schultz

September 1995

Prepared for
the U.S. Department of Energy
under Contract DE-AC06-76RLO 1830

Pacific Northwest Laboratory
Richland, Washington 99352

Executive Summary

A software package, Sectoral Energy/Employment Analysis and Data System (SEADS-PC), that can translate policy changes into employment and energy impacts is described. The core data for this tool include input-output (I/O) tables for 1977, 1982, 1987, and 2005 in 1982 dollars, and I/O tables for 1987 and 1990 in 1987 dollars. For each of the I/O tables there are corresponding final demand vectors and employment intensities. For all but the 2005 table there are energy intensities as well. The final demands and the intensities can be changed to reflect alternative policies. A final demand vector that reflects a specific policy, for example, can be created, based on an existing final demand vector. This vector can then be premultiplied by the appropriate I/O table to yield industry output, which in turn can be multiplied by energy or employment intensities to yield employment or energy resulting from the policy scenario. These policy results can then be compared with a base case and the differences reported.

The report is in four sections. The first section is an introduction. The second section provides the accounting framework for the tool and describes the data provided. The third section serves as a user's guide to the software, describing the functionality of the program and what results can be expected. The fourth section uses the President's Climate Change Action Plan (CCAP) as an example policy for which employment impacts can be calculated.

The results of the CCAP exercise suggest that this program will result in about 60,000 new jobs (about 115 million additional hours of work) for the year 2000. In the year 2000, the CCAP final demands are greater than the base case final demands by $192.8 million (1990 dollars). The additional jobs are created as a result of both the shifts among final demand categories and a slight increase in economic activity.

Acronymns

BEA Bureau of Economic Analysis
BLS Bureau of Labor Statistics

CCAP Climate Change Action Plan

DRI Data Resources, Inc.

EIA Energy Information Administration

GDP Gross Domestic Product

I/O Input-output

MECS Manufacturing Energy Consumption Survey

OMB Office of Management and Budget

SEADS Sectoral Energy/Employment Analysis and Data System
SIC Standard Industrial Classification

48-750 98 - 4

Acknowledgments

This document is a major revision of a program first developed by David B. Belzer in the mid-1980s; his contribution is gratefully acknowledged. The authors would also like to thank our U.S. Department of Energy sponsor, Peggy Podolak, Office of Economic Policy and Competition, (202) 586-6430, without whose support this work would not have been accomplished. Thanks also to Steve Shankle for his suggestions and comments, and to Susan Ennor for her editorial assistance.

Inquiries about SEADS-PC should be addressed to Joseph M. Roop, Pacific Northwest Laboratory, P.O. Box 999, MSIN: K8-17, Richland, WA 99352 (509) 372-4245.

Contents

Figure

Tables

1.0 Introduction

This guide was written by staff of the Pacific Northwest Laboratory[a] for users of the SEADS-PC (Sectoral Energy/Employment Analysis and Data System) for IBM-compatible computers using Windows. SEADS is designed to show the employment and energy implications of changing the industrial structure and patterns of final demands for goods within the U.S. economy.

This version of SEADS-PC is a Windows-based program, written in VisualBasic with extensive documentation provided through help documents. This user's guide provides instructions for preparing various scenarios with the system and walks the user through a typical exercise of running a scenario and preparing tables and spreadsheets. The example used to demonstrate the analytical tool is a comparison of a Climate Change Action Plan scenario with a base case forecast for the year 2000.

SEADS contains core data for analysis for four base years: 1977, 1982, 1987, and 1990. The core data include a vector of final demands, an input-output table, energy intensities, and labor intensities. A set of multipliers that convert national labor and hours data from the national to the state level is also available and can be applied to all core data sets. Input-output, final demand, and employment (i.e., labor intensity) data are also available for the Bureau of Labor Statistics (BLS) forecast year 2005 (BLS 1993). Forecasts of Gross Domestic Product (derived from the U.S. Department of Energy's subscription to Data Resources, Inc. forecasts) between 1995 and 2010 are provided at five-year intervals, with the capability of bridging from these forecasts to a vector of final demands that can generate outputs for analysis. The example analysis is done using both the current (i.e., 1990) industry structure and the industry structure represented by the BLS 2005 input-output table.

This report is organized into three additional sections. The next section provides the accounting framework for the analytical tool and describes the data that constitute the core data set provided with the model. The third section describes the capabilities of SEADS and indicates how the tool can be used to examine a variety of questions that bear on energy policy. The final section demonstrates the analytical power of the tool by applying it to the Climate Change Action Plan.

(a) The Pacific Northwest Laboratory is operated by the Battelle Memorial Institute for the U.S. Department of Energy under Contract DE-AC06-76 RLO 1830.

2.0 Methodology and Data

2.1 Basic Accounting Structure

The basic input-output (I/O) accounting structure employed in SEADS, along with the employment and energy calculations, are shown in Figure 2.1. The box at the top of the figure is optional. The Data Resources, Inc. (DRI) forecasts (the example is for 1995) are converted through a bridge matrix to a vector of final demands. Alternatively, the user could start with one of the provided final demand vectors. The sum of all final demands is the Gross Domestic Product (GDP). The selected or constructed final demands are pre-multiplied by the total requirements matrix (labeled "Input-Output Table") to yield industry output for each of the 85 industries. This total output for each industry is shown as the box labeled "Industry Output." From a cost perspective total output for each *industry* must equal the cost of purchased commodities plus value added. Value added consists of payments to primary factors — labor compensation, capital or profit-type income, and indirect business taxes. These outputs are not available separately, but are intermediate in the calculation of jobs and hours or energy use.

Employment intensity is shown in the box labeled, "Jobs and Hours Intensities" beneath the output box. These intensities were calculated by dividing jobs or hours for each of the 85 industries by output. Thus these intensities represent the jobs or hours per dollar of output for each of the industries for which output is calculated.

Energy intensity is defined in terms of Btu/per dollar of output, analogous to employment intensities. These intensities are also shown in the figure as an alternative path. Like employment, there is no single intensity for each industry; rather, in SEADS intensities are defined for four fuel types—coal, oil, natural gas, and electricity. Energy use, is computed as the product of output times intensity, on an industry-by-industry basis for each fuel. Similarly, employment (i.e., jobs and hours) is computed as the product of output times employment intensity, on an industry-by-industry basis, and this is shown in the figure. SEADS also provides an option to define a subregion of the United States for which employment (but not energy) impacts can be determined. These regional impacts are calculated by sharing the nation impacts down to the state (or regional) level. This is shown as an option in Figure 2.1.

Figure 2.1 helps to provide some perspective of the relationship between the composition of GDP and employment or energy use in the economy. One of the key capabilities in SEADS is the ability to calculate employment based on an arbitrary set of final demands. By itself, Figure 2.1 does not spell out how this procedure is performed. For this, a more detailed explanation, in terms of the basic matrix algebra underlying the I-O method employed in SEADS, is provided below.

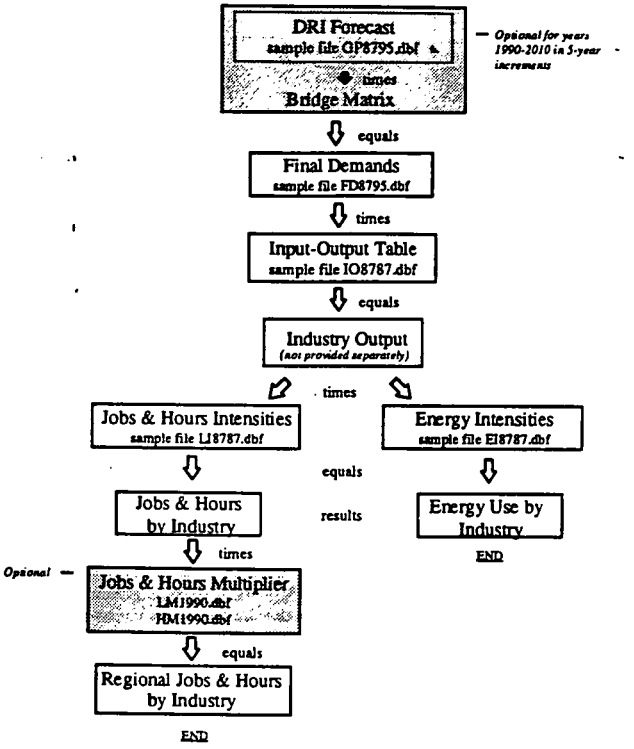

Figure 2.1. The Determination of Employment Using the SEADS-PC Approach

2.2 Final Demand

We begin first with the determination of final demands by commodity. Let F be a column vector of total final demand by commodity. In SEADS we follow the Bureau of Economic Analysis (BEA) convention of reporting 85 commodities and industries, as listed in Section 2.7 (BEA 1991). In terms of Figure 2.1, Final Demands is a 85x1 vector that is the *row* sums of the various components, including personal consumption expenditures, business investment components, and other final demand components. In SEADS a forecast set of GDP components can be converted to this final demand vector and used to generate employment impacts. There are 29 of these final forecast demand categories, as shown in Table 2.1.

Table 2.1. GDP Components

No.	Sector
1	C-Motor Vehicles
2	C-Furniture & Appliances
3	C-Other Durables
4	C-Food & Beverages
5	C-Clothing & Shoes
6	C-Gasoline & Oil
7	C-Fuel Oil & Coal
8	C-Other Nondurables
9	C-Housing Services
10	C-Household Electric Services
11	C-Household Natural Gas Services
12	C-Other Household Services
13	C-Transportation Services
14	C-Medical Services
15	C-Other Services
16	I-Nonresidential Equipment
17	I-Nonresidential Structures
18	I-Residential Structures
19	I-Residential Equipment
20	I-Manufacturing Inventory Change
21	I-Retail Trade Inventory Change
22	I-Wholesale Trade Inventory Change
23	I-Other Nonfarm Inventory Change
24	I-Farm Inventory Change
25	Exports
26	Imports
27	G-National Defense
28	G-Federal Nondefense
29	G-State & Local Government
C: Consumption I: Investment G: Government	

For an I/O application, there must be an industrial distribution of final demand categories with entries for each of the 85 rows of the final demand array in Figure 2.1. Thus, to convert from these 29 forecast categories to the 85 industries, a "bridge" is used. For example, for category 16, Nonresidential Equipment (Producers Durable Equipment), there would be non-zero row entries corresponding to a number of producing sectors, including machine tools, motor vehicles, other transportation equipment, etc. Let matrix H represent this distribution after normalization to a per-dollar-of-final-demand basis. That is, an element of H, h_{ij}, represents the amount of commodity i sold per dollar's worth of final demand category j. Because this distribution is fairly stable over time, one can translate a given vector of GDP final demand categories into a vector of commodity demands via the matrix expression.

$$F = HG \tag{2.1}$$

The dimension of H in SEADS is 85x29. H is commonly referred to as a bridge matrix, because it is used to bridge between the GDP category and commodity levels of final demand.

2.3 Industry Output

The next step is to compute the levels of output that would be required to satisfy the final demands by commodity (F). In *standard* I/O analysis, the fundamental identity is

$$X_c = AX_c + F \tag{2.2}$$

where: A = an nxn matrix of direct requirements coefficients,
X_c = an nx1 vector of outputs, and
F = an nxl vector of final demands.

A is defined on a commodity-by-commodity basis, where a_{ij} represents the amount of commodity i required in the production of a dollar's worth of commodity j. From Equation (2.2), the solution for F is obtained by:

$$X_c = (I-A)^{-1}F \tag{2.3}$$

$(I-A)^{-1}$ is commonly known as the Leontief inverse.

This simple solution to Equation (2.2) is based on the existence of a commodity-to-commodity direct requirements table, A. Such a table is not published as part of the official I/O accounts for the United States. Rather, the U.S. Department of Commerce in the 1972 and subsequent input-output studies has released two separate tables, a "use" table and "make" table. The use table shows the value of each commodity *used* by each industry. The make table, on the other hand, shows the value of each commodity *produced* by each industry.

By using the use and make matrices, some organizations have generated estimates of commodity-by-commodity tables for the 1972 and 1977 U.S. input- output studies. SEADS, however, has followed an alternative approach used by the U.S. Department of Commerce (BEA 1994). This approach employs what is termed an industry-technology assumption, which assumes that industries employ commodities in fixed proportion to their total *industry* (rather than commodity) output. To determine industry output, a second assumption must also be made, namely that the market shares by each industry in the production of a specific commodity remain constant.

The derivation of the solution for industry output using these assumptions is somewhat tedious and will not be given here. The final result is:

$$X = D\,(I-BD)^{-1}F \qquad (2.4)$$

where: I = the identity matrix
X = a vector of industry outputs
F = a vector of final demands by commodity
D = an industry-by-commodity matrix in which entries in each column show for a given commodity the proportion of total output of that commodity produced in each industry. D is referred to as the market share matrix, and is constructed from the Make matrix.
B = a commodity-by-industry matrix in which entries in each column show the amount of a commodity used by an industry per dollar of output of that industry. This is constructed from the Use matrix.

In the development of this version of SEADS, the matrix $D(I-BD)^{-1}$ for all core years except 1982 was computed from the use and make matrices provided by the Long-Term Growth Project of the BLS. For 1982, the official benchmark table was used. A benchmark table for 1987 is also provided. This total requirements matrix is represented by the box labeled "Input-Output Table" in Figure 2.1.

The core data include four BLS total requirements matrices in 1982 dollars and two BLS matrices in 1987 dollars. The BLS tables in 1987 dollars were developed using the 1982 Standard Industrial Classification (SIC) definitions, which were significantly revised with the publication of the 1987 benchmark I/O table. Constant dollar tables are needed for comparison through time, so we have provided the BLS tables. The benchmark 1987 table is also provided, although this table is not comparable with the other tables because of the SIC changes.

2.4 Energy Intensities

The computation of energy intensities was straightforward. Energy-use data by industry and fuel were taken from the National Energy Accounts (NEA; Jack Faucett Associates 1989), which contain data for the period from 1958 to 1985. Fuel types were aggregated to four major categories: coal, natural gas, oil and electricity. The industry data were converted to the BEA industries using a concordance based on SIC codes (Office Management Budget [OMB] 1987). Data for 1987 and 1990 were constructed to match with the Manufacturing Energy Consumption Survey (MECS) data for manufacturing for 1988 (Energy Information

Administration [EIA] 1991) and 1991 (EIA 1994), and for other industries based on Annual Survey (Bureau of the Census 1992) and Census (Bureau of the Census 1990) data.

To generate historical energy intensities, historical output data were taken from the Office of Economic Growth in the BLS. After aggregation to the BEA basis, the outputs were scaled to match the industry outputs from the core year I/O table. Intensities for each fuel type were then computed as simply the energy use by industry sector divided by the industry output.

SEADS-PC saves the results of calculating the projected or simulated energy use by industry. In matrix notation the energy-use matrix is calculated as:

$$E = e.X \tag{2.5}$$

where: E = energy use, with dimension: industry x fuel type
e = a matrix of energy intensities (for a specific year) of dimension fuel type x industry
. = a dot product operation, i.e., X is diagonalized before matrix multiplication.

Using the matrix E, energy consumption for any desired aggregation of industries can be easily calculated. A similar set of intensities for jobs and hours allows for the computation of labor use based on generated industry output.

2.5 Relation of Equation Variables to SEADS Variables

To go from the 29 final demand categories (G) to the matrix of energy use/employment by industry the complete procedure in SEADS requires the calculation of F (Equation 1), then the following matrix expression:

$$E = e.\ [D\ (I-BD)^{-1}]\ F \tag{2.6}$$

In the instructions that follow in the next section, the user will generally select a set of these various components in Equation (2.6) to perform a wide variety of analyses. In addition to selecting these files, the user may wish to edit any of the various arrays for which editing is allowed to tailor the analysis to some special purpose applications. For employment impacts rather than energy impacts, there is a third set of variables: an employment multiplier that allows the translation from national employment impacts to state-level impacts. To facilitate these applications, the SEADS variables corresponding to these components are listed in Table 2.2 (a single bridge matrix is provided by the program—it is contained in a file called BRIDGE.DBF).

2.6 The Core Data Set

The data that have been constructed for SEADS include I/O tables for a variety of years, energy intensities for most of the years, labor intensities for these years, and final demands for the core set of

Table 2.2. Correspondence Between Variables and Data Files

Matrix/Vector	SEADS	Description
G	gp1987.dbf	GDP Components, 1987
F	fd1987.dbf	Aggregate Final Demand, 1987
$D(I-BD)^{-1}$	io1987.dbf	Input-Output Table for 1987
e	ei1987.dbf	Energy Intensity for 1987
l	li1987.dbf	Labor Intensities for 1987
lm	lm1990.dbf	Jobs Multiplier
hm	hm1990.dbf	Hours Multiplier

years. There are seven I/O tables: for 1977, 1982, 1987 and 2005, all in 1982 constant dollars (naming convention: "io1987.dbf"); and for 1987 and 1990 in 1987 dollars ("io8787.dbf" and "io8790.dbf") based on the 1982 SIC definitions; and the benchmark 1987 table ("io87bm.dbf"). There are also seven final demand vectors with similar naming conventions (i.e., "fd1977.dbf" for $1982; "fd8790.dbf" for $1987, and "fd87bm.dbf" for the benchmark final demands) and seven labor intensities (prefix "li") similarly named. There are only six energy intensity files (prefix "ei"), matched to all except the 2005 data, for which there are no adequate forecasts. There is only one file for each of the labor and hours multipliers (prefixes "lm" and "hm") for 1990. These files share the national totals to the state level and are constructed for only one year. A bridge matrix is also provided, "bridge.dbf" based on the 1987 final demands, that maps from the gp files to the fd files. Experiments with the 1977 and 1987 data suggest that this bridge does not change significantly over time.

2.7 Industry Classification

The industry classification used in this version of SEADS-PC is one that is used by the BEA, U.S. Department of Commerce, and it might be termed the standard I/O (85-Sector) classification. This classification is shown in Table 2.3, and is based on the 1982 SIC (BEA 1991). The sector classification changed substantially in 1987; we have retained the 1982 industry definitions.

Table 2.3. Industry Sectors in SEADS[a]

No./ Industry	
1 Livestock and livestock products	44 Farm and garden mach.
2 Other agri. products	45 Construction and mining mach.
3 Forestry and fishery products	46 Materials handling mach. and equip.
4 Agri., forestry, and fishery serv.	47 Metalworking mach. and equip.
5 Iron and ferroalloy ore mining	48 Special industry mach. and equip.
6 Nonferrous metal ore mining	49 General industrial mach. and equip.
7 Coal mining	50 Misc. mach. except elec.
8 Crude petroleum and natural gas	51 Office, computing, and accounting equip.
9 Stone and clay mining and quarrying	52 Serv. industry machines
10 Chem & fertilizer mineral mining	53 Elec. industrial equip. and apparatus
11 New construction	54 Household appliances
12 Maintenance and repair construction	55 Elec. lighting and wiring equip.
13 Ordinance and accessories	56 Radio, TV, and communications equip.
14 Food and kindred products	57 Elec. components and accessories
15 Tobacco	58 Misc. elec. mach. and supplies
16 Broad and narrow fabrics	59 Motor vehicles and equip.
17 Misc. textiles and flooring	60 Aircraft and parts
18 Apparel	61 Other transportation equip.
19 Misc. fabricated textiles	62 Scientific and controlling instr.
20 Lumber and wood products	63 Optical, ophthalmic, and photo equip.
21 Wood containers	64 Misc. mfg.
22 Household furniture	65 Transportation and warehousing
23 Other furniture and fixtures	66 Communications, except radio and TV
24 Paper and allied products	67 Radio and TV broadcasting
25 Paperboard containers and boxes	68 Elec., gas, water, and sanitary serv.
26 Printing and publishing	69 Trade
27 Chemicals and selected products	70 Finance and insurance serv.
28 Plastics and synthetic materials	71 Real estate
29 Drugs, cleaning and toilet prep.	72 Hotel and lodging serv.
30 Paints and allied products	73 Business serv.
31 Petroleum refining industries	74 Eating and drinking places
32 Rubber and misc. plastics	75 Automobile repair serv.
33 Leather tanning and finishing	76 Amusements
34 Footwear and other leather products	77 Health, education, and social serv.
35 Glass and glass products	78 Federal government enterprise
36 Stone and clay products	79 State and local government enterprise
37 Primary iron and steel mfg.	80 Noncomparable imports
38 Primary nonferrous metal mfg.	81 Scrap
39 Metal containers	82 Government industry
40 Fabricated structural metal products	83 Rest of the world industry
41 Screw machine prod and stampings	84 Household industry
42 Other fabricated metal products	85 Inventory valuation adjustment
43 Engines and turbines	

(a) agri. = agricultural; elec. = electrical; equip. = equipment; instr. = instruments; mach. = machinery; mfg. = manufacturing; misc. = miscellaneous; prep. = preparations; serv. = services.

48-750 98 - 5

3.0 SEADS-PC Capabilities

Installation of SEADS-PC makes various program options and computational capabilities available to you, as described in the following sections.

3.1 Installation

SEADS-PC is installed by following the instruction in the READ.ME file that comes with the SEADS diskettes. The installation kit includes two diskettes. The first of these is put into the diskette drive (A:\, for example), and the Run option is selected under the File selection under Program Manager. The Run command would be A:SETUP. The data files are loaded by copying all of the core files from the subdirectory A:\DBF to a similar subdirectory under the SEADS directory.

3.2 Program Options

SEADS-PC includes the use of various screens and options that are described here.

SEADS Screen. Once installed, the program is invoked by double-clicking on the SEADS icon. The opening window of SEADS has six options on the options bar at the top of the screen, but under the title bar. The Select Files options allows you to load files for each of the bulleted items show in the middle of the screen. The Edit File option allows you to edit selected files. The New and Save As... options allow you to copy and rename existing files to modify them. The Set Defaults option establishes a set of selected files as the default files to load whenever SEADS is invoked; and the Exit option returns you to the Windows Program Manager.

The major part of the opening screen is a matrix with three column headings and three major row headings. The columns are labeled File Type, Selected Files/Options, and Computational Options. The headings that define the major rows are labeled Macro Specification, Energy Specifications, and Labor Specifications. Under the File Type column and in the Macro Specification row, three files types are identified—GDP, Final Demand, and I/O Table. Once a set of default files has been identified, these are loaded automatically and will be identified under the second column. If these are blank, the user should invoke Select Files to identify a set of files to work with. There are two function buttons under the first column labeled FUEL TYPE and LABOR REGION. The first allows you to choose the set of fuels you wish to include in the analysis; the second allows you to specify a region or state to examine for employment impacts. The second column will identify what options are chosen using these buttons; the defaults are all fuel types and the entire Unites States.

Under the third column are three buttons that perform the calculations for the SEADS tool. The first of these, labeled GENERATE FINAL DEMAND performs the calculation shown in Equation 2.1. Using a bridge matrix, it maps from the 29 components of GDP to the 85-component final demand vector. When this option is invoked, SEADS will ask for a file name for the newly created file. The second button, labeled COMPUTE

ENERGY USE, performs the calculation of Equation (2.5), where e is energy intensity. Progress during these calculations is indicated on a overlay screen. The third button is labeled COMPUTE LABOR USE, and this button calculates Equation (2.5) using labor and hours intensities rather than energy intensities. Further, if a region or a state has been selected, the results for the United States will be shared down to the state or region based on state level employment information by industry. If the default is used, there is no need for this sharing down to occur. This computation also reports progress with an indicator.

If a region or state is selected, the mouse is clicked on the LABOR REGION button and a map of the United States (sans Hawaii, which will be included in the next release) appears. Buttons on the right-hand side of the map provide six pre-defined regions: WESTERN, EASTERN, CENTRAL, GREAT LAKES, COASTAL, and ENTIRE U.S. Below these regions are two additional buttons, a CLEAR ALL button that clears all current specified states/regions, and an OK button that returns you to the main program. When you first enter this map, all states are displayed in yellow, indicating that the default, Entire U.S., is currently invoked. By clicking on a state, that state changes color, indicating that a new region has been defined, consisting of all states except the one on which you clicked. To define a particular region, first hit CLEAR ALL, then click on the states of interest. When these are colored and the remainder of the map is not, you have specified a Custom Region, which will be indicated in the box under the second column headings when you return to the main menu. If you wish to delete a state from a Custom Region, just click on it a second time and it will be removed from that user-defined region.

Select Files Screen. When you select this option, a File Selector screen appears that shows the files currently selected, the directory and files within which you are operating (usually C:\SEADS\DBF*.*) and three buttons: SELECT, CLEAR, and RETURN. To the left of the selected files is a column of file types, with bullet-like buttons on the extreme left. By selecting a bullet, a black dot will fill the bullet, indicating that you are doing something with this type of file. For example, if you select Final Demand, you could clear the current file or you could identify a file from those shown in the File Names section to use for this exercise. Final demand files are identified by the fd prefix, then a year, then the extension dbf. So if you identify "fd1987.dbf" from the file names, then click on the SELECT button, that file will appear in the Selected Files area for that file type. Because each file type has a predefined form, you will receive an error message if you select an incorrect file type. When all necessary files for your analysis are selected, click on the RETURN button and the program reverts to the SEADS main menu.

Edit File Screen. When you invoke the Edit File option from the main menu, the editor will load the file currently identified by the highlighted button to the left of the selected file. If you wish to edit the final demand vector that you create from a GDP forecast, invoke this option with the highlighted button on the created file, and the next screen you see will be a standard Windows edit screen with the operating cell where changes are made at the top of the editor. The remainder of the screen is filled with three columns: the first column contains the number of the sector; the second contains the title for this sector, and the third contains the values currently in the aggregate final demand vector. If you want to change the current value for row 35, Glass and Glass Products, simply 1) click on that cell, which loads row 35 into the editor, 2) click on the edit cell and make changes in the edit box, and 3) hit Enter. When all editing is complete, you can save the file

under its current name or a different name (the Save or Save As... options). The Cancel option restores the file to its original state. The Units option tells the user the units for the current numbers. Finally, the Return option returns you to the main menu. If you have not saved the file, your changes will not be saved.

New and Save As... Screens. Both of these options invoke the New File Name menu screen, which either allows you to substitute a new file for the current file identified with the highlighted bullet or save that file under a different name.

Set Defaults Screen. Once a set of files has been selected, using this option will identify this set of files as the one you want to load the next time you enter SEADS.

Exit Option. This option returns computer control to the Windows Program Manager.

3.3 Computation of Labor and Energy Impacts

When either the COMPUTE ENERGY USE or the COMPUTE LABOR USE buttons are invoked at the main menu, Equation (2.5) is computed with the files that were identified. When the calculation is complete, the results are shown on the next screen. These results can be saved under a new name, printed, or compared with a prior run; the units used can be shown, a summary table of the results can be shown, or you can return to the main menu. These are in the options bar at the top of the page and their functions are described here.

Save As... Option. This invokes the New Name screen and allows you to save results under a different name, and it is identical to the same option under the main menu. When a file is saved, it is saved under a *.dbf format, with a corresponding file with a *.dbs designation. This latter file contains all relevant information about what files were used to produce this result and the date and time of the run.

Print Option. This option allows you to print either to a printer (the Windows default) or to a file. If the Print-to-File option is selected, the results will be printed to a text file that a can then be accessed by a word processing package. When you print to a file, the relevant data contained in the *.dbs file will be printed along with the results.

Compare Option. With this option, you can compare the current results with results obtained from a prior run. Just identify the previously named file and these two files will be compared. The Results screen is similar to the Energy (Employment) Results screen, except that now both the results and the differences are shown on the screen. You can scroll down to the bottom of the results to see the total impact. The Save As... option here is the same as it is on the Results screen.

Summary Option. This option can be invoked from either the Results screen or the Compare screen. The Results Summary would show energy use by fuel type for the entire economy and energy use by major sectors—Agriculture, Mining, Construction, Manufacturing, Services, Other, and Total—for each fuel. From the comparison option, these headings would show both scenarios and the difference between the two. When the Summary Print-to-File option is employed, these final results, along with the two scenario descriptions, are all printed to the file name that you identify.

Units and Return Options The Units option is the same as it is in the Edit File menu. The Return option returns to the SEADS main menu.

3.4 SEADS and Spreadsheets

SEADS is designed to be used with any of the major spreadsheet programs currently available under Windows—Quattro Pro, Lotus 1-2-3, or Excel. Any of these packages will read and write *.dbf files, making it easy to structure special analytical files. Most users will find it more convenient to structure analysis files in a spreadsheet environment than to use the editor provided in SEADS. Because all files are stored in dBase format, it is important that revisions to existing files preserve the structure of the original dBase files. The most efficient way to ensure this is to copy the appropriate set of numbers from a working spreadsheet, close the spreadsheet file, then paste these numbers into a template for the appropriate file. The naming convention for a template is ??_FORM.DBF, where ?? will be FD, EI, or any other label that is allowed. Be sure that when you save this file you do not overwrite the template. The template files are stored in the C:\SEADS directory. An example of how this is done is provided in the next section. In addition, if the comparison of results is to be shown, it is necessary to read in the results.dbf files and take the differences between these two files to show as a comparison file.

4.0 An Example Application: The Climate Change Action Plan

This section describes how to perform an analysis with the SEADS-PC system, using as an example the President's proposed Climate Change Action Plan (CCAP). More detailed tables and results files are in the Appendix.

4.1 Final Demand Changes

For this analysis, two final demand vectors were provided: one a base case for the year 2000, the other the same final demands under the CCAP. Table 4.1 shows the summary results file saved during a comparison between the base case and CCAP case using the I/O table for 2005 and employment intensities for 2005.

Table 4.1. Summary Results File Showing Comparison Between Base Case and CCAP Case (Using I/O table and Employment Intensities for 2005)

Specifications and Results: Date: 01-25-1995 Time: 17:19:23
Case 1 specifications: GDP: C:\SEADS\DBF\GP1990.DBF Final demand: C:\SEADS\DBF\FDD2000B.DBF IO table: C:\SEADS\DBF\IO2005.DBF Energy intensity: C:\SEADS\DBF\EI1990.DBF Labor intensity: C:\SEADS\DBF\LI2005.DBF Jobs multiplier: C:\SEADS\DBF\LM1990.DBF Hours multiplier: C:\SEADS\DBF\HM1990.DBF Labor region: US
Results: Labor use
Results units: Jobs – Millions Hours – Millions
Case 2 specifications Date: 01-25-1995 Time: 11:02:29
Case files selected: GDP:\ Final Demand: C:\SEADS\DBF\FDD2000C.DBF IO table: C:\SEADS\DBF\IO2005.DBF Energy intensity: C:\SEADS\DBF\EI1990.DBF Labor intensity: C:\SEADS\DBF\LI2005.DBF Jobs multiplier: C:\SEADS\DBF\LM1990.DBF Hours multiplier: C:\SEADS\DBF\HM1990.DBF Labor region: US

The difference between these two scenarios (in 1990 dollars) is shown in Table 4.2. Overall there is very little difference between these final demand vectors, with the difference for all industries adding up to only $192.8 million, with CCAP expenditures slightly higher by that amount. While this sum is small, there are some large differences between the two scenarios for some categories of final demand. The largest of these are for new construction (larger under CCAP by $2.3 billion), petroleum refining (lower under CCAP by nearly $2.8 billion), and electric and gas utility sales (lower under CCAP by $3.8 billion). The decline in energy sales through these two major sectors are compensated for by smaller changes in many other industries.

These final demand changes are both in 1990 dollars, so the first task was to convert these to 1982 dollars (the constant dollar value for the 2005 I/O table). To convert the final demand vectors to 1982 dollars the output deflators were first converted to final demand deflators by postmultiplying the output deflators by the inverse of the total requirements matrix, as given in Equation 2.4.[a] This vector of final demand deflators was then multiplied, element by element, by both the CCAP and the 2000 base final demand vectors. Then both of these deflated final demand vectors were run through SEADS using both the 1990 and the 2005 I/O tables to conduct the analysis. The deflation procedure reduces the value of the final demand vector from $6.25 trillion to almost $5 trillion and reduces the CCAP expenditures so that they are now smaller than the base case by $886 million. These differences are shown in Appendix A, Table A.5.

4.2 CCAP Labor Impacts: The Procedure

Eight runs were performed to assess the employment impact of the President's CCAP. SEADS was employed for both the base case and the CCAP final demands using two different sets of I/O tables (1990 and 2005) and two sets of labor intensities (again 1990 and 2005). The results were saved as *.dbf files and the comparisons were saved as print files that contain information about the runs, an example of which is shown in Table 4.1. Table 4.3 was constructed by loading the results files into Lotus 1-2-3, copying the information, closing the file, then pasting the data to a standard *.wk3 file. (This procedure is necessary in Lotus, because the template for an *.dbf file will override the calculations and only part of the data will be saved, even if the file is saved using the Save As... option.) Results from each of the *.dbf files for the eight runs was likewise copied to a spreadsheet, then organized to be written to a disk file for loading into WordPerfect. All of the files included in this analysis are included with the installation kit, so that any or all of the results can be duplicated.

(a) The same relationship holds between the output deflator and the final demand deflator as holds for output and final demand in Equation 2.4. Because BLS supplies the output deflators (1982 = 100) for each year from 1958 to 1990, it is a simple matter to take the output deflator for 1990, substitute the deflator series for X in Equation 2.4, then solve the equation for the final demand deflators by premultiplying each side of the equation by the inverse of the total requirements matrix. The result is the final demand deflator that was applied to the CCAP and base case final demands.

Table 4.2. Base Case and CCAP Final Demands

No./Industry Description	Base 2000	CCAP 2000	Difference
1-6 Six Industries	45562.9	45579.6	-16.7
7 Coal mining	5363.7	5316.9	46.8
8-10 Three Industries	-41440.6	-41440.1	-0.5
11 New construction	512510.1	514858.5	-2348.4
12 Maintenance and repair construction	60522.3	60633.2	-110.9
13 Ordinance and accessories	23217.8	23171.6	46.2
14 Food and kindred products	249208.2	249279.0	-70.8
15-21 Seven Industries	94242.9	94307.9	-65.0
22 Household furniture	21587.7	21693.1	-105.4
23 Other furniture and fixtures	24570.7	24689.3	-118.6
24 Paper and allied products	21213.2	21015.7	197.5
25-30 Six Industries	140481.9	140566.0	-84.1
31 Petroleum refining industries	58993.8	56237.3	2756.5
32-50 Nineteen Industries	154106.3	154677.3	-541.0
51 Office, computing, and accounting equipment	161818.9	162165.3	-346.4
52 Service industry machines	16141.2	16205.4	-64.2
53 Electric industrial equipment and apparatuses	10394.2	10507.7	-113.5
54 Household appliances	18686.2	18757.9	-71.7
55 Electric lighting and wiring equipment	3619.2	3632.9	-13.7
56 Radio, TV, and communications equipment	35124.0	35521.3	-397.3
57 Electronic components and accessories	4740.9	4608.4	132.5
58 Misc. electrical machinery and equipment	25372.9	25432.6	-59.7
59 Motor vehicles and equipment	185378.9	185670.2	-291.3
60 Aircraft and parts	107893.6	107916.0	-22.4
61 Other transportation equipment	27720.4	27800.8	-80.4
62 Scientific and controlling instruments	78954.1	79048.0	-93.9
63 Optical, ophthalmic, and photography equipment	19736.7	19827.1	-90.4
64 Miscellaneous manufacturing	25368.0	25421.5	-53.5
65 Transportation and warehousing	178391.7	178466.7	-75.0
66 Communications, except radio and TV	119583.3	119729.3	-146.0
67 Radio and TV broadcasting	19559.2	19559.4	-0.2
68 Electric, gas, water, and sanitary services	142219.8	138416.4	3803.4
69 Trade	925122.3	926096.5	-974.2
70 Finance and insurance services	306537.5	306620.1	-82.6
71 Real estate	575473.4	575880.3	-406.9
72-76 Five Industries	617145.7	617250.9	-105.2
77 Health, education, and social services	740964.0	741166.9	-202.9
78-85 Nine Industries	537882.7	537875.7	7.0
TOTALS	6253970.0	6254162.8	-192.8

Table 4.3. Summary of Findings (Various I/O and Labor Intensity Assumptions [In millions except Jobs Difference in units])

Year	Base Case	CCAP Case	Difference	Base Case	CCAP Case	Difference
	Labor Intensity 1990			Labor Intensity 2005		
			Total Jobs			
1990 I/O	127.226	127.273	-47,400	130.284	130.340	-56,600
2005 I/O	126.075	126.135	-60,100	127.237	127.307	-69,500
			Total Hours			
1990 I/O	239435.12	239522.79	- 87.67	250256.86	250367.86	-111.00
2005 I/O	237674.25	237786.59	-112.34	244523.11	244658.63	-135.52

4.3 Labor Impacts: Results

The results of the eight sets of calculations are shown Table 4.3. In all cases the results are strikingly similar. Under the total jobs section of the summary findings, there is a difference between the Base Case and the CCAP case of between -47,400 and -69,500 jobs; the lower number is derived when the 1990 I/O and 1990 labor intensity are used, the higher when both the 2005 I/O and labor intensity are used. This means that there are between 47,000 and 70,000 more jobs under the CCAP case than under the base case. These results suggest that the CCAP will account for about 60,000 new jobs or about 115 million more hours worked per year in the year 2000.

The astute reader will notice that the calculations using the I/O table for 1990 should have used final demand vectors in 1987 dollars, because the I/O table is in those units, not in the vectors defined in 1982 dollars. This would give rise to some bizarre results except for the fact that the labor intensities are also defined in 1987 dollars. The same calculation using the 1990 I/O table (in 1987 dollars) and labor intensities for 1990 (again in 1987 dollars) but using the final demand vectors defined as in Table 4.2 (in 1990 dollars) provides differences that are nearly identical to the results using the I/O table and the labor intensities for 2005. Total jobs under CCAP, for example, are 69,800 more than under the base case (compared to 69,500) and hours increase by 130 million rather than the 135.5 million reported above.

5.0 References

Bureau of the Census. See U.S. Department of Commerce. Bureau of the Census.

Bureau of Economic Analysis (BEA). See U.S. Department of Commerce, Bureau of Economic Analysis.

Bureau of Labor Statistics. See U.S. Department of Labor, Bureau of Labor Statistics.

Energy Information Administration. See U.S. Department of Energy, Energy Information Administration.

Jack Faucett Associates. 1989. *National Energy Accounts 1958-1985*. JACFAU-89-351. Jack Faucett Associates, Bethesda, Maryland.

Office of Management and Budget. 1987. *Standard Industrial Classification Manual*. National Technical Information Service, Springfield, Virginia.

U.S. Department of Commerce, Bureau of the Census. 1992. *1990 Annual Survey of Manufacturers. Statistics for Industry Groups and Industries*. M90(AS)-1. United States Government Printing Office, Washington, D.C. (Available for various, non-census years.)

U.S. Department of Commerce, Bureau of the Census. 1990. *1987 Census of Manufacturers. Industry Series*. MC87-I-20D. United States Government Printing Office, Washington, D.C. (Available every five years.)

U.S. Department of Commerce, Bureau of Economic Analysis. 1991. "Benchmark Input-Output Accounts of the United States, 1982." *Survey of Current Business*. July (71:7), pp. 30-71.

U.S. Department of Commerce, Bureau of Economic Analysis. 1994. *Benchmark Input-Output Accounts of the United States, 1987*. U.S. Government Printing Office, Washington, D.C.

U.S. Department of Energy, Energy Information Administration (EIA). 1991. *Manufacturing Energy Consumption Survey: Consumption of Energy, 1988*. DOE/EIA-0512(88). Washington, D.C.

U.S. Department of Energy, Energy Information Administration (EIA). 1994. *Manufacturing Consumption of Energy, 1991*. DOE/EIA-0512(91). Washington, D.C.

U.S. Department of Labor, Bureau of Labor Statistics, Office of Employment Projections. 1993. *OUTLOOK: 1992-2005: Input-Output 228 Order Diskette Documentation*. Washington, D.C.

Appendix

Selected Detailed Tables and Results Files for the Example Application: Employment Implications of the Climate Change Action Plan

Appendix

Selected Detailed Tables and Results Files for the Example Application: Employment Implications of the Climate Change Action Plan

This appendix contains detailed print-outs for the comparison of the two final demand cases using the 1990 table and intensity and for the two cases using the 2005 table and intensity. The first two tables (A.1 and A.2) show the detailed results from these two comparisons. The second set of tables (A.3 and A.4) shows a typical comparison when you request that the results be saved to a file (only the summary results are shown here; the detailed results may also be printed). Finally, Table A.5 shows the details of the base case and CCAP final demand vectors in 1990 dollars, the differences, the values deflated to 1982 dollars, and the final demand deflator.

Table A.1. Base Case Jobs and Hours Compared to Climate Change Action Plan

I/O 1990 for both Base and CCAP LI 1990 for both Base and CCAP							
		Base Case		CCAP		Difference	
No.	Industry	Jobs	Hours	Jobs	Hours	Jobs	Hours
1	Livestock	1.4174	3220.843	1.4177	3221.683	-0.0003	-0.8398
2	Other agr	1.144	2517.607	1.1443	2518.271	-0.0003	-0.6636
3	Forestry	0.0731	162.5146	0.0732	162.6707	-1.0E-04	-0.1561
4	Agricultu	0.4703	1029.944	0.4706	1030.518	-0.0003	-0.5735
5	Iron and	0.0272	59.6033	0.0272	59.6644	0	-0.0611
6	Nonferrou	0.0032	6.996	0.0032	7.0067	0	-0.0107
7	Coal mini	0.0818	183.7563	0.081	181.9393	0.0008	1.817
8	Crude pet	0.0612	131.0846	0.058	124.1343	0.0032	6.9503
9	Stone and	0.0494	112.9234	0.0494	112.8748	0	0.0486
10	Chemical	0.0024	5.6175	0.0024	5.616	0	0.0015
11	New const	0.5175	1163.919	0.5193	1167.906	-0.0018	-3.9872
12	Maintenan	0.0166	37.7441	0.0166	37.7148	0	0.0293
13	Ordinance	0.3054	639.464	0.3049	638.4256	0.0005	1.0384
14	Food and	3.2646	6871.332	3.2654	6873.034	-0.0008	-1.7022
15	Tobacco	0.039	79.9334	0.039	79.947	0	-0.0136
16	Broad and	0.3306	691.8021	0.3309	692.456	-0.0003	-0.6539
17	Misc. tex	0.1519	327.7877	0.1523	328.566	-0.0004	-0.7783
18	Apparel	1.7981	3454.363	1.7988	3455.693	-0.0007	-1.3304
19	Misc. fab	0.3312	669.8539	0.3315	670.3784	-0.0003	-0.5245
20	Lumber an	0.5826	1218.192	0.5839	1220.802	-0.0013	-2.6103
21	Wood cont	0.0071	14.9265	0.0071	14.9538	0	-0.0273
22	Household	0.7125	1436.383	0.7159	1443.251	-0.0034	-6.8677
23	Other fur	0.4985	1036.973	0.5007	1041.578	-0.0022	-4.6052
24	Paper and	0.286	633.4821	0.2855	632.3783	0.0005	1.1038
25	Paperboar	0.1853	404.2308	0.1853	404.3112	0	-0.0804
26	Printing	1.5587	3146.577	1.5594	3147.985	-0.0007	-1.4087
27	Chemicals	0.3352	730.9066	0.3349	730.2413	0.0003	0.6653
28	Plastics	0.1624	350.4167	0.1625	350.6212	-1.0E-04	-0.2045
29	Drugs, cl	0.6059	1277.181	0.6059	1277.047	0	0.1342
30	Paints an	0.054	114.7288	0.0541	114.8597	-0.0001	-0.1309
31	Petroleum	0.2832	631.699	0.276	615.7584	0.0072	15.9406
32	Rubber an	0.6887	1459.93	0.6892	1461.148	-0.0005	-1.2175
33	Leather t	0.0045	9.138	0.0047	9.5779	-0.0002	-0.4399
34	Footwear	0.1053	207.184	0.1056	207.6977	-0.0003	-0.5137

Table A.1. (contd)

I/O 1990 for both Base and CCAP LI 1990 for both Base and CCAP							
		Base Case		CCAP		Difference	
No.	Industry	Jobs	Hours	Jobs	Hours	Jobs	Hours
35	Glass and	0.1471	315.178	0.1472	315.4381	-0.0001	-0.2601
36	Stone and	0.4055	873.5022	0.4062	874.9788	-0.0007	-1.4766
37	Primary i,	0.3699	810.9413	0.3703	811.8192	-0.0004	-0.8779
38	Primary n	0.3595	778.3444	0.36	779.5193	-0.0005	-1.1749
39	Metal con	0.0558	125.5973	0.0557	125.4882	0.0001	0.1091
40	Fabricate	0.4591	968.9094	0.4599	970.6609	-0.0008	-1.7515
41	Screw mac	0.3055	655.1812	0.3058	655.9042	-0.0003	-0.723
42	Other fab	0.4369	924.5176	0.4376	925.9562	-0.0007	-1.4386
43	Engines a	0.1233	266.7726	0.1233	266.7395	0	0.0331
44	Farm and	0.2401	512.1072	0.241	514.0291	-0.0009	-1.9219
45	Construct	0.2924	635.4653	0.2928	636.4799	-0.0004	-1.0146
46	Materials	0.1294	274.294	0.1298	275.1289	-0.0004	-0.8349
47	Metalwork	0.112	243.2275	0.1132	245.9061	-0.0012	-2.6786
48	Special i	0.2568	547.3252	0.2575	548.9184	-0.0007	-1.5932
49	General i	0.6846	1472.572	0.6856	1474.78	-0.001	-2.2089
50	Misc. mac	0.104	224.2609	0.1042	224.5347	-0.0002	-0.2738
51	Office, c	3.7615	7971.841	3.7692	7988.171	-0.0077	-16.3301
52	Service i	0.2427	504.9201	0.2433	506.3255	-0.0006	-1.4054
53	Electric	0.3254	695.6024	0.3266	698.1318	-0.0012	-2.5294
54	Household	0.2834	581.7142	0.2844	583.7535	-0.001	-2.0393
55	Electric	0.1708	355.2979	0.1711	355.9763	-0.0003	-0.6784
56	Radio, TV	0.5528	1176.484	0.5579	1187.21	-0.0051	-10.7255
57	Electroni	0.6914	1439.685	0.6921	1441.065	-0.0007	-1.3799
58	Misc. ele	0.3653	774.9645	0.366	776.4367	-0.0007	-1.4722
59	Motor veh	1.8964	4117.941	1.899	4123.624	-0.0026	-5.6826
60	Aircraft	1.9991	4256.481	1.9995	4257.239	-0.0004	-0.7583
61	Other tra	0.5134	1067.588	0.5147	1070.276	-0.0013	-2.6883
62	Scientifi	1.1895	2493.895	1.1907	2496.374	-0.0012	-2.4793
63	Optical,	0.2149	451.4417	0.2155	452.6247	-0.0006	-1.183
64	Miscellan	0.5816	1200.571	0.5825	1202.468	-0.0009	-1.8973
65	Transport	3.4534	6969.996	3.4517	6966.486	0.0017	3.5098
66	Communica	0.883	1873.344	0.8837	1874.744	-0.0007	-1.4001
67	Radio and	0.6573	1229.124	0.6574	1229.351	-1.0E-04	-0.2271
68	Electric,	0.8984	1947.051	0.8856	1919.358	0.0128	27.6936
69	Trade	24.9764	43739.29	24.9975	43776.13	-0.0211	-36.8398

Table A.1. (contd)

I/O 1990 for both Base and CCAP LI 1990 for both Base and CCAP							
		Base Case		CCAP		Difference	
No.	Industry	Jobs	Hours	Jobs	Hours	Jobs	Hours
70	Finance a	5.2902	10020.91	5.2901	10020.62	0.0001	0.2881
71	Real esta	1.2943	2483.634	1.2943	2483.719	0	-0.0845
72	Hotel and	3.5591	6280.34	3.5599	6281.831	-0.0008	-1.4908
73	Business	7.9556	14779.42	7.9577	14783.34	-0.0021	-3.9228
74	Eating an	8.232	11053.06	8.2322	11053.32	-0.0002	-0.2588
75	Automobil	1.7769	3485.847	1.7772	3486.432	-0.0003	-0.5852
76	Amusement	1.2449	1953.017	1.2452	1953.439	-0.0003	-0.4223
77	Health, e	19.3815	33291.92	19.3864	33300.3	-0.0049	-8.3789
78	Federal g	0.5881	1228.148	0.5878	1227.565	0.0003	0.5823
79	State and	1.0437	2213.289	1.0414	2208.417	0.0023	4.8728
80	Noncompar	0	0	0	0	0	0
81	Scrap	0	0	0	0	0	0
82	Governmen	12.563	26131.02	12.563	26131.02	0	0
83	Rest of t	0	0	0	0	0	0
84	Household	0	0	0	0	0	0
85	Inventory	0	0	0	0	0	0
86	Total	127.2258	239435.1	127.2732	239522.7	-0.0474	-87.671

Table A.2. Base Case Jobs and Hours Compared to Climate Change Action Plan

I/O 2005 for Both Base and CCAP LI 2005 for both Base and CCAP							
		Base Case		CCAP		Difference	
No.	Industry	Jobs	Hours	Jobs	Hours	Jobs	Hours
1	Livestock	2.4997	5679.011	2.5005	5680.668	-0.0008	-1.6568
2	Other agr	2.6411	5811.958	2.6419	5813.693	-0.0008	-1.7349
3	Forestry	0.2778	617.1246	0.2781	617.8082	-0.0003	-0.6836
4	Agricultu	1.5565	3407.973	1.5575	3410.187	-0.001	-2.2139
5	Iron and	0.0221	48.4385	0.0221	48.5104	0	-0.0719
6	Nonferrou	0.0022	5.0185	0.0022	5.0289	0	-0.0104
7	Coal mini	0.1269	286.4341	0.1258	283.8192	0.0011	2.6149
8	Crude pet	0.0768	163.9854	0.0751	160.2155	0.0017	3.7699
9	Stone and	0.0274	62.6111	0.0274	62.6335	0	-0.0224
10	Chemical	0.0034	7.8244	0.0034	7.8282	0	-0.0038
11	New const	5.2229	11857.38	5.2392	11894.41	-0.0163	-37.0322
12	Maintenan	0.5303	1163.758	0.5301	1163.416	0.0002	0.3425
13	Ordinance	0.1239	254.7377	0.1237	254.3299	0.0002	0.4078
14	Food and	1.2915	2714.343	1.2919	2715.092	-0.0004	-0.7493
15	Tobacco	0.0222	45.4138	0.0222	45.4214	0	-0.0076
16	Broad and	0.3461	723.7605	0.3464	724.4883	-0.0003	-0.7278
17	Misc. tex	0.099	213.376	0.0992	213.8897	-0.0002	-0.5137
18	Apparel	0.4944	949.9213	0.4946	950.2973	-0.0002	-0.376
19	Misc. fab	0.107	216.6199	0.1071	216.7955	-0.0001	-0.1756
20	Lumber an	1.1696	2508.202	1.1721	2513.505	-0.0025	-5.303
21	Wood cont	0.0165	34.8027	0.0165	34.8678	0	-0.0651
22	Household	0.2229	449.51	0.224	451.6324	-0.0011	-2.1224
23	Other fur	0.1474	306.7733	0.1481	308.1426	-0.0007	-1.3693
24	Paper and	0.4501	998.0058	0.4497	997.0176	0.0004	0.9882
25	Paperboar	0.1686	367.8141	0.1687	368.0372	-1.0E-04	-0.2231
26	Printing	1.3436	2712.461	1.3444	2714.109	-0.0008	-1.6475
27	Chemicals	0.3322	724.245	0.3321	724.2108	0.0001	0.0342
28	Plastics	0.1464	315.8497	0.1465	316.1121	-0.0001	-0.2624
29	Drugs, cl	0.3296	694.9766	0.3297	695.0552	-0.0001	-0.0786
30	Paints an	0.0538	114.2356	0.0538	114.3841	0	-0.1485
31	Petroleum	0.1289	285.3006	0.1267	280.4814	0.0022	4.8192
32	Rubber an	0.2706	544.8731	0.2709	545.4358	-0.0003	-0.5627
33	Leather t	0.0009	1.7864	0.0009	1.8741	0	-0.0877
34	Footwear	0.0017	3.4015	0.0017	3.4097	0	-0.0082

Table A.2. (contd)

I/O 2005 for Both Base and CCAP LI 2005 for both Base and CCAP							
		Base Case		CCAP		Difference	
No.	Industry	Jobs	Hours	Jobs	Hours	Jobs	Hours
35	Glass and	0.0073	15.68	0.0073	15.7016	0	-0.0216
36	Stone and	0.0858	141.4406	0.086	141.7089	-0.0002	-0.2683
37	Primary i	3.394	7253.293	3.399	7263.929	-0.005	-10.6362
38	Primary n	1.5485	3405.981	1.5513	3411.951	-0.0028	-5.9698
39	Metal con	0.0393	88.5409	0.0393	88.5198	0	0.0211
40	Fabricate	0.4598	970.2691	0.4608	972.3594	-0.001	-2.0903
41	Screw mac	0.2578	553.2466	0.2581	553.8946	-0.0003	-0.648
42	Other fab	0.438	926.9031	0.4388	928.7079	-0.0008	-1.8048
43	Engines a	0.1206	260.6893	0.1206	260.6629	0	0.0264
44	Farm and	0.1451	309.503	0.1456	310.6912	-0.0005	-1.1882
45	Construct	0.1754	381.2212	0.1757	381.9181	-0.0003	-0.6969
46	Materials	0.0998	211.5132	0.1001	212.172	-0.0003	-0.6588
47	Metalwork	0.0972	207.9142	0.0983	210.354	-0.0011	-2.4398
48	Special i	0.2	426.1737	0.2006	427.5222	-0.0006	-1.3485
49	General i	0.6325	1356.26	0.6336	1358.486	-0.0011	-2.2264
50	Misc. mac	0.0202	43.7117	0.0202	43.755	0	-0.0433
51	Office, c	1.6885	3673.286	1.6919	3680.789	-0.0034	-7.5027
52	Service i	0.0956	199.1913	0.0959	199.7387	-0.0003	-0.5474
53	Electric	0.0731	153.844	0.0734	154.5062	-0.0003	-0.6622
54	Household	0.0642	131.9769	0.0644	132.4409	-0.0002	-0.464
55	Electric	0.0947	196.9264	0.0949	197.3066	-0.0002	-0.3802
56	Radio, TV	0.1416	301.5116	0.1428	303.9682	-0.0012	-2.4566
57	Electroni	0.254	529.4594	0.2543	529.9376	-0.0003	-0.4782
58	Misc. ele	0.0991	210.4862	0.0993	210.8669	-0.0002	-0.3807
59	Motor veh	2.0031	4238.751	2.006	4244.815	-0.0029	-6.0644
60	Aircraft	1.6215	3451.833	1.6218	3452.483	-0.0003	-0.6504
61	Other tra	0.2648	551.928	0.2655	553.3797	-0.0007	-1.4517
62	Scientifi	0.7445	1558.647	0.7453	1560.308	-0.0008	-1.6608
63	Optical,	0.157	329.4598	0.1574	330.3468	-0.0004	-0.887
64	Miscellan	0.1863	384.7673	0.1866	385.3927	-0.0003	-0.6254
65	Transport	3.1368	6334.903	3.1369	6335.017	-0.0001	-0.1143
66	Communica	0.9852	2090.239	0.986	2092.006	-0.0008	-1.7675
67	Radio and	0.2731	510.8904	0.2732	511.0763	-1.0E-04	-0.1859
68	Electric,	0.9137	1983.075	0.9009	1955.405	0.0128	27.6702
69	Trade	27.201	47620	27.2264	47664.54	-0.0254	-44.5313

Table A.2. (contd)

I/O 2005 for Both Base and CCAP LI 2005 for both Base and CCAP							
		Base Case		CCAP		Difference	
No.	Industry	Jobs	Hours	Jobs	Hours	Jobs	Hours
70	Finance a	5.2157	9876.104	5.2161	9876.783	-0.0004	-0.6797
71	Real esta	1.4022	2686.099	1.4025	2686.789	-0.0003	-0.6897
72	Hotel and	2.8896	5098.724	2.8904	5100.151	-0.0008	-1.4278
73	Business	10.5324	19566.24	10.5378	19576.2	-0.0054	-9.9609
74	Eating an	6.0702	8152.157	6.0708	8153.048	-0.0006	-0.8911
75	Automobil	1.6548	3245.479	1.6553	3246.392	-0.0005	-0.9133
76	Amusement	1.5881	2492.312	1.5886	2493.016	-0.0005	-0.7041
77	Health, e	11.4852	19735.91	11.4884	19741.28	-0.0032	-5.3672
78	Federal g	0.2718	567.6454	0.2718	567.6885	0	-0.0431
79	State and	1.2967	2749.393	1.2952	2746.201	0.0015	3.1921
80	Noncompar	0	0	0	0	0	0
81	Scrap	0	0	0	0	0	0
82	Governmen	16.8543	35057.61	16.8543	35057.61	0	0
83	Rest of t	0	0	0	0	0	0
84	Household	0	0	0	0	0	0
85	Inventory	0	0	0	0	0	0
86	Total	127.2374	244523.1	127.3067	244658.6	-0.0695	-135.5

Table A.3. Typical Comparison of the 2000 Base Case With 2000 CCAP Final Demands Results Saved to a File (Using 1990 Input-Output Table and Intensity)

Specifications and Results:
Date: 08-14-1995
Time: 16:46:39
Case 1 specifications:
GDP: C:\SEADS\DBF\GP1990.DBF
Final demand: C:\SEADS\DBF\FDD2000B.DBF
IO table: C:\SEADS\DBF\CORE\IO8790.DBF
Energy intensity: C:\SEADS\DBF\CORE\EI1987.DBF
Labor intensity: C:\SEADS\DBF\CORE\LI8790.DBF
Jobs multiplier: C:\SEADS\DBF\LM1990.DBF
Hours multiplier: C:\SEADS\DBF\HM1990.DBF
Labor region: US
Results: Labor use
Results units:
Jobs -- Millions
Hours -- Millions
Case 2 specifications:
Date: 08-14-1995
Time: 11:02:11
Case files selected:
GDP: C:\SEADS\DBF\GP1990.DBF
Final demand: C:\SEADS\DBF\FDD2000C.DBF
IO table: C:\SEADS\DBF\CORE\IO8790.DBF
Energy intensity: C:\SEADS\DBF\EIDUM.DBF
Labor intensity: C:\SEADS\DBF\CORE\LI8790.DBF
Jobs multiplier: C:\SEADS\DBF\LM1990.DBF
Hours multiplier: C:\SEADS\DBF\HM1990.DBF
Labor region: US
Results: Labor use

Table A.3. (contd)

Summary Results:			
	Case 1	Case 2	Difference
Jobs	1.27E+02	1.27E+02	-4.74E-02
Hours	2.39E+05	2.40E+05	-8.77E+01
Industry	Jobs 1	Jobs 2	Jobs Diff.
Agriculture	3.10E+00	3.11E+00	-1.00E-03
Mining	2.25E-01	2.21E-01	4.00E-03
Construction	5.34E-01	5.36E-01	-1.80E-03
Manufacturing	2.96E+01	2.96E+01	-3.53E-02
Services	4.87E+01	4.87E+01	-8.50E-03
Other	4.51E+01	4.51E+01	-4.80E-03
Total	1.27E+02	1.27E+02	-4.74E-02
Industry	Hours 1	Hours 2	Hours Diff.
Agriculture	6.93E+03	6.93E+03	-2.23E+00
Mining	5.00E+02	4.91E+02	8.75E+00
Construction	1.20E+03	1.21E+03	-3.96E+00
Manufacturing	6.21E+04	6.22E+04	-7.36E+01
Services	8.33E+04	8.34E+04	-1.49E+01
Other	8.53E+04	8.53E+04	-1.81E+00
Total	2.39E+05	2.40E+05	-8.77E+01

Table A.4. Typical Comparison of the 2000 Base Case with 2000 CCAP Results Saved to a File (Using 2005 Input-Output Table and Intensity)

Specifications and Results: Date: 08-14-1995 Time: 16:44:52
Case 1 specifications: GDP: C:\SEADS\DBF\GP1990.DBF Final demand: C:\SEADS\DBF\FDD2000B.DBF IO table: C:\SEADS\DBF\CORE\IO2005.DBF Energy intensity: C:\SEADS\DBF\CORE\EI1987.DBF Labor intensity: C:\SEADS\DBF\CORE\LI2005.DBF Jobs multiplier: C:\SEADS\DBF\LM1990.DBF Hours multiplier: C:\SEADS\DBF\HM1990.DBF Labor region: US
Results: Labor use
Results units: Jobs -- Millions Hours -- Millions
Case 2 specifications: Date: 08-14-1995 Time: 10:06:46
Case files selected: GDP: C:\SEADS\DBF\GP1990.DBF Final demand: C:\SEADS\DBF\FDD2000C.DBF IO table: C:\SEADS\DBF\CORE\IO2005.DBF Energy intensity: C:\SEADS\DBF\EIDUM.DBF Labor intensity: C:\SEADS\DBF\CORE\LI2005.DBF Jobs multiplier: C:\SEADS\DBF\LM1990.DBF Hours multiplier: C:\SEADS\DBF\HM1990.DBF Labor region: US
Results: Labor use

Table A.4. (contd)

Summary Results:			
	Case 1	Case 2	Difference
Jobs	1.27E+02	1.27E+02	-6.93E-02
Hours	2.45E+05	2.45E+05	-1.36E+02
Industry	Jobs 1	Jobs 2	Jobs Diff.
Agriculture	6.98E+00	6.98E+00	-2.90E-03
Mining	2.59E-01	2.56E-01	2.80E-03
Construction	5.75E+00	5.77E+00	-1.61E-02
Manufacturing	2.25E+01	2.25E+01	-2.95E-02
Services	4.08E+01	4.08E+01	-1.17E-02
Other	5.09E+01	5.09E+01	-1.21E-02
Total	1.27E+02	1.27E+02	-6.93E-02
Industry	Hours 1	Hours 2	Hours Diff.
Agriculture	1.55E+04	1.55E+04	-6.29E+00
Mining	5.74E+02	5.68E+02	6.28E+00
Construction	1.30E+04	1.31E+04	-3.67E+01
Manufacturing	4.76E+04	4.77E+04	-6.24E+01
Services	7.09E+04	7.09E+04	-2.06E+01
Other	9.69E+04	9.69E+04	-1.58E+01
Total	2.45E+05	2.45E+05	-1.36E+02

Table A.5. Final Demands for the Climate Change Action Plan Analysis (1990 Dollar Values in Millions, Deflator, and 1982 Dollar Values in Millions.)

No.	Industry description	Base	CCAP	Diff	Deflator	Deflated FD, 2000		
						Base	CCAP	Diff
1	Livestock and livestock products	4793.43	4794.83	-1.40	1.07	4459.84	4461.14	-1.30
2	Other agricultural products	41867.98	41877.08	-9.10	1.18	35505.41	35513.13	-7.72
3	Forestry and fishery products	-2106.40	-2109.10	2.70	1.32	-1598.66	-1600.71	2.05
4	Agricultural, forestry, and fishery services	1544.02	1548.02	-4.00	1.20	1281.99	1285.31	-3.32
5	Iron and ferroalloy ore mining	-472.20	-472.20	0.00	0.92	-515.78	-515.78	0.00
6	Nonferrous metal ore mining	-63.90	-59.00	-4.90	0.92	-69.80	-64.44	-5.35
7	Coal mining	5363.75	5316.95	46.80	0.82	6551.71	6494.54	57.17
8	Crude petroleum and natural gas	-41222.60	-41222.60	0.00	0.72	-63147.37	-63147.37	0.00
9	Stone and clay mining and quarrying	-215.60	-215.90	0.30	1.18	-183.47	-183.73	0.26
10	Chemical and fertilizer mineral mining	-2.40	-1.60	-0.80	1.18	-2.04	-1.36	-0.68
11	New construction	512510.15	514858.55	-2348.40	1.21	423492.11	425432.61	-1940.51
12	Maintenance and repair construction	60522.28	60633.18	-110.90	1.24	48643.53	48732.66	-89.13
13	Ordinance and accessories	23217.83	23171.63	46.20	1.10	21189.95	21147.78	42.16
14	Food and kindred products	249208.18	249278.98	-70.80	1.22	203451.85	203509.66	-57.80
15	Tobacco	20723.17	20726.57	-3.40	2.08	9985.15	9986.78	-1.64
16	Broad and narrow fabrics	598.48	599.38	-0.90	1.14	525.90	526.69	-0.79
17	Misc. textiles and flooring	8410.83	8440.53	-29.70	1.17	7192.43	7217.83	-25.40
18	Apparel	52395.53	52415.03	-19.50	1.15	45676.51	45693.51	-17.00
19	Misc. fabricated textiles	10619.60	10626.40	-6.80	1.11	9560.31	9566.43	-6.12
20	Lumber and wood products	1410.62	1415.32	-4.70	1.32	1070.93	1074.49	-3.57
21	Wood containers	84.68	84.68	0.00	1.21	70.23	70.23	0.00
22	Household furniture	21587.74	21693.14	-105.40	1.25	17253.62	17337.86	-84.24
23	Other furniture and fixtures	24570.68	24689.28	-118.60	1.32	18635.33	18725.28	-89.95
24	Paper and allied products	21213.15	21015.65	197.50	1.32	16092.52	15942.69	149.83
25	Paperboard containers and boxes	1839.91	1840.61	-0.70	1.32	1396.52	1397.05	-0.53
26	Printing and publishing	41592.93	41633.63	-40.70	1.44	28833.92	28862.13	-28.21
27	Chemicals and selected products	16188.23	16199.13	-10.90	1.15	14060.82	14070.29	-9.47
28	Plastics and synthetic materials	8948.05	8948.05	0.00	1.22	7356.18	7356.18	0.00
29	Drugs, cleaning and toilet preparations	70455.57	70485.87	-30.30	1.39	50603.73	50625.49	-21.76
30	Paints and allied products	1457.19	1458.69	-1.50	1.28	1140.66	1141.83	-1.17
31	Petroleum refining industries	58993.81	56237.31	2756.50	0.79	74911.82	71411.55	3500.27
32	Rubber and misc. plastics	13402.52	13411.32	-8.80	1.17	11468.87	11476.40	-7.53
33	Leather tanning and finishing	10.41	30.81	-20.40	1.44	7.24	21.44	-14.20
34	Footwear and other leather products	1829.71	1834.71	-5.00	1.35	1354.54	1358.24	-3.70
35	Glass and glass products	2702.98	2718.58	-15.60	1.19	2266.08	2279.15	-13.08
36	Stone and clay products	1732.65	1743.45	-10.80	1.15	1509.14	1518.55	-9.41
37	Primary iron and steel mfg	-9043.92	-9044.02	0.10	1.18	-7636.51	-7636.60	0.08
38	Primary nonferrous metal mfg	-1498.19	-1495.49	-2.70	1.33	-1129.43	-1127.40	-2.04
39	Metal containers	357.30	357.70	-0.40	1.12	318.34	318.69	-0.36
40	Fabricated structural metal products	7922.64	7947.14	-24.50	1.21	6525.52	6545.70	-20.18

Table A.5. (contd)

No.	Industry description	Base	CCAP	Diff	Deflator	Deflated FD, 2000		
						Base	CCAP	Diff
41	Screw machine products and stampings	5232.25	5231.65	0.60	1.18	4420.62	4420.11	0.51
42	Other fabricated metal products	6490.94	6537.54	-46.60	1.25	5210.26	5247.67	-37.41
43	Engines and turbines	9812.06	9825.56	-13.50	1.25	7869.79	7880.62	-10.83
44	Farm and garden machinery	18562.49	18641.79	-79.30	1.21	15297.92	15363.27	-65.35
45	Construction and mining machinery	22992.41	23052.81	-60.40	1.16	19752.93	19804.82	-51.89
46	Materials handling machinery and eq.	7769.14	7800.54	-31.40	1.16	6718.97	6746.12	-27.16
47	Metalworking machinery and equipment	4851.28	4944.48	-93.20	1.22	3981.36	4057.85	-76.49
48	Special industry machinery and eq.	21071.27	21154.97	-83.70	1.30	16223.64	16288.09	-64.44
49	General industrial machinery and eq.	37848.29	37922.59	-74.30	1.24	30633.98	30694.12	-60.14
50	Misc. machinery except electrical	2060.26	2061.26	-1.00	1.22	1690.26	1691.08	-0.82
51	Office, computing, and accounting eq.	161818.93	162165.33	-346.40	0.46	353108.28	353864.17	-755.89
52	Service industry machines	16141.20	16205.40	-64.20	1.23	13164.67	13217.03	-52.36
53	Electric industrial eq and apparatus	10394.19	10507.69	-113.50	1.23	8438.21	8530.35	-92.14
54	Household appliances	18686.25	18757.95	-71.70	1.14	16459.30	16522.46	-63.16
55	Electric lighting and wiring equipment	3619.18	3632.88	-13.70	1.27	2846.39	2857.16	-10.77
56	Radio, TV, and communications eq.	35124.02	35521.32	-397.30	1.10	32012.41	32374.51	-362.10
57	Electronic components and accessories	4740.89	4608.39	132.50	1.05	4533.26	4406.57	126.70
58	Misc. electrical machinery and supplies	25372.86	25432.56	-59.70	1.10	22995.16	23049.27	-54.11
59	Motor vehicles and equipment	185378.92	185670.22	-291.30	1.17	158389.37	158638.26	-248.89
60	Aircraft and parts	107893.63	107916.03	-22.40	1.21	88874.49	88892.94	-18.45
61	Other transportation equipment	27720.35	27800.75	-80.40	1.26	22070.35	22134.36	-64.01
62	Scientific and controlling instruments	78954.08	79047.98	-93.90	1.21	65245.91	65323.51	-77.60
63	Optical, ophthalmic, and photographic eq.	19736.75	19827.15	-90.40	1.11	17709.06	17790.17	-81.11
64	Miscellaneous manufacturing	25368.01	25421.51	-53.50	1.20	21152.34	21196.95	-44.61
65	Transportation and warehousing	178391.72	178466.72	-75.00	1.23	145128.31	145189.33	-61.02
66	Communications, except radio and TV	119583.31	119729.31	-146.00	1.34	89227.95	89336.89	-108.94
67	Radio and TV broadcasting	19559.21	19559.41	-0.20	1.44	13583.73	13583.87	-0.14
68	Electric, gas, water, and sanitary services	142219.80	138416.40	3803.40	1.15	124057.75	120740.06	3317.69
69	Trade	925122.29	926096.49	-974.20	1.20	771128.03	771940.06	-812.04
70	Finance and insurance services	306537.50	306620.10	-82.60	1.46	210562.92	210619.66	-56.74
71	Real estate	575473.37	575880.27	-406.90	1.48	388439.67	388714.32	-274.65
72	Hotel and lodging services	95509.66	95535.06	-25.40	1.50	63736.84	63753.79	-16.95
73	Business services	172884.08	172927.28	-43.20	1.53	113181.07	113209.35	-28.28
74	Eating and drinking places	181197.35	181202.25	-4.90	1.34	135211.81	135215.47	-3.66
75	Automobile repair services	107780.05	107799.55	-19.50	1.39	77612.19	77626.23	-14.04
76	Amusements	59774.54	59786.74	-12.20	1.42	42097.71	42106.30	-8.59
77	Health, education, and social services	740963.98	741166.88	-202.90	1.53	483594.82	483727.24	-132.42
78	Federal government enterprise	11354.57	11361.37	-6.80	1.34	8484.96	8490.04	-5.08

Table A.5. (contd)

No.	Industry description	Base	CCAP	Diff	Deflator	Deflated FD, 2000		
						Base	CCAP	Diff
79	State and local government enterprise	19623.23	19626.13	-2.90	1.48	13302.98	13304.95	-1.97
80	Noncomparable imports	-41844.00	-41860.70	16.70	0.00	0.00	0.00	0.00
81	Scrap	-18255.30	-18255.30	0.00	0.00	0.00	0.00	0.00
82	Government industry	567003.99	567003.99	0.00	1.49	380974.26	380974.26	0.00
83	Rest of the world industry	0.20	0.20	0.00	0.00	0.00	0.00	0.00
84	Household industry	0.00	0.00	0.00	1.10	0.00	0.00	0.00
85	Inventory valuation adjustment	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	TOTALS	6253970	6254162.8	-192.8		4997233.6	4996347.3	886.3199

PNL-10760
UC-98F

Distribution

No. of Copies

Offsite

2 DOE/Office of Scientific and Technical Information (OSTI)

20 P. Podolak
U.S. Department of Energy
Office of Economic Analysis and Competition
Mail Stop PO-61
Washington, D.C. 20585

B. Card
U.S. Department of Energy
Office of Planning and Assessment
Mail Stop EE-70
Washington, D.C. 20585

E. Petersen
U.S. Department of Energy
Office of Planning and Assessment
Mail Stop EE-70
Washington, D.C. 20585

No. of Copies

Onsite

32 Pacific Northwest Laboratory

D. M. Anderson
W. B. Ashton
D. B. Belzer
A. K. Nicholls
J. M. Roop (25)
R. W. Schultz
M. J. Scott
M. G. Woodruff

Appendix C

Post-Bid Scenario Table

Case Study

Post-Bid Scenario Table

	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
2	Product sales, units		1995 unit	value	$51,000			Royalty	4%		1.0	0.8	0.6	0.3	0.1	
3	Year	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	Total
4	Base forecast															
5	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
6	Government	2,500	2,200	1,800	1,700	1,783	2,300	3,000	3,800	3,800	3,600	2,700	2,025	1,013	338	32,138
7	Initial Contract															
8	Other Government	2,500	2,200	1,800	1,700	1,783	2,300	3,000	3,800	3,800	3,600	2,700	2,025	1,013	338	32,138
9	Foreign Civilian	10	50	101	126	400	800	800	850	1,020	800	624	468	234	78	6,361
10	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
11	U.S. Government	18,000	12,000	9,000	3,000	2,350	2,350	2,350	2,350	3,400	3,400	2,720	2,040	1,020	340	61,320
12	Civilian	303	350	400	1,240	1,263	1,650	2,500	3,000	3,000	3,000	2,028	1,521	761	254	21,269
13	Individual	303	333	360	1,054	1,074	1,320	1,875	2,100	1,950	1,800	1,056	792	396	132	14,544
14	Bulk	-	18	40	186	189	330	625	900	1,050	1,200	972	729	365	122	6,725
15	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
16	U.S. units/day	76	62	48	26	25	29	37	42	47	46	34	26	13	4	
17	Property loss forecast															
18	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
19	Government	2,500	2,200	1,800	1,700	1,783	2,070	2,550	2,880	2,700	2,520	1,755	1,215	557	169	26,379
20	Initial Contract															
21	Other Government	2,500	2,200	1,800	1,700	1,783	2,070	2,550	2,880	2,700	2,520	1,755	1,215	557	169	26,379
22	Foreign Civilian	10	50	101	126	400	570	510	375	325	275	200	150	75	25	3,192
23	[illegible]ic - Total	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
24	U.S. Government	18,000	12,000	9,000	3,000	2,350	2,350	2,350	2,350	3,400	3,400	2,720	2,040	1,020	340	61,320
25	Civilian	303	350	400	1,240	1,263	1,650	2,500	3,000	2,505	2,370	1,517	1,022	439	146	18,706
26	Individual	303	333	360	1,054	1,074	1,320	1,875	2,100	1,560	1,350	739	475	198	66	12,806
27	Bulk	-	18	40	186	189	330	625	900	945	1,020	778	547	241	80	5,898
28	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
29	U.S. units/day	76	62	48	26	25	28	34	37	38	36	26	19	9	3	
30	Net forecast															
31	Foreign	0	0	0	0	0	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
32	Government	0	0	0	0	0	-230	-450	-720	-900	-1,080	-945	-810	-456	-169	-5,759
33	Initial Contract	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
34	Other Government	0	0	0	0	0	-230	-450	-720	-900	-1,080	-945	-810	-456	-169	-5,759
35	Foreign Civilian	0	0	0	0	0	-30	-290	-675	-695	-825	-424	-318	-159	-53	-3,169
36	Domestic - Total	0	0	0	0	0	0	0	0	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
37	U.S. Government	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
38	Civilian	0	0	0	0	0	0	0	0	-495	-630	-511	-499	-322	-107	-2,564
39	Individual	0	0	0	0	0	0	0	0	-390	-450	-317	-317	-198	-66	-1,738
40	Bulk	0	0	0	0	0	0	0	0	-105	-180	-194	-182	-124	-41	-827
41	[illegible]	0	0	0	0	0	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
42	U.S. units/day	0	0	0	0	0	-1	-3	-6	-9	-10	-8	-7	-4	-1	
43	Table 6 continued. Post-Bid Scenario															
44	National impacts															
45	Year	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	Total
46	Trade, $M	0	0	0	0	0	-15	-42	-74	-120	-134	-108	-83	-54	-19	-659
47	Royalties $M	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
48	Taxes(payroll), $M	0	0	0	0	0	-1	-3	-6	-9	-10	-8	-7	-4	-1	-49
49	Taxes(corp), $M	0	0	0	0	0	-1	-4	-6	-10	-11	-9	-8	-6	-2	-56
50	[illegible] jobs	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
51	Company jobs	0	0	0	0	0	-54	-155	-271	-437	-488	-393	-340	-196	-69	-2,402
52	Supplier jobs	0	0	0	0	0	-88	-250	-438	-706	-789	-635	-550	-316	-111	-3,884
53	Indirect jobs	0	0	0	0	0	-43	-122	-213	-344	-384	-309	-268	-154	-54	-1,892
54																
55	Company impacts															
56	Year	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	
57	Revenue, $M	0	0	0	0	0	-13	-38	-66	-107	-119	-96	-83	-48	-17	-586
58	Net income	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	-82
59	Royalties $M	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
60	Profits(sales), $M	0	0	0	0	0	-2	-6	-10	-16	-17	-14	-12	-7	-2	-86
61	Profits(margin), $M	0	0	0	0	0	0	-1	-2	-3	-3	-2	-2	-1	0	-14
62	Taxes, $M	0	0	0	0	0	1	2	4	7	8	6	5	3	1	38
63	Company jobs	0	0	0	0	0	-54	-155	-271	-437	-488	-393	-340	-196	-69	-2,402
64																
65																
66	Supplier impacts															
67	Year	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	
68	Revenue, $M	0	0	0	0	0	-9	-27	-47	-76	-85	-68	-59	-34	-12	-419
69	Profits(sales), $M	0	0	0	0	0	-1	-3	-6	-10	-11	-9	-7	-4	-1	-52
70	Taxes, $M	0	0	0	0	0	0	1	2	3	4	3	3	1	1	18
71	Supplier jobs	0	0	0	0	0	-88	-250	-438	-706	-789	-635	-550	-316	-111	-3,884
72	Indirect jobs	0	0	0	0	0	-43	-122	-213	-344	-384	-309	-268	-154	-54	-1,892

Case Study

Table Notes:

Note: Because of rounding, figures may not add to the totals shown.

Total column (R): This is the sum of 1992 through 2005.

Base Forecast (lines 4-16): This section presents the original forecast, given no loss of IP.

Initial contract (line 7): Figures for initial contract represent sales under the initial contract. These figures are not included in the total (line 15) or in the calculation for U.S. units/day.

Total (line 15): Sum of foreign (line 5) and domestic (line 10) sales for any given year. Totals for 1992 - 1996 are based on actual sales. Totals for 1997 - 2005 are forecasted sales.

U.S. units/day (line 16): This is the number of units produced daily in order to fill any one year's worth of orders (line 15.) U.S. units per day is calculated using a one-shift, 235-day work year.

IP Theft Forecast (lines 17-29): This section presents the revised forecast, given a theft of IP.

Net Forecast (lines 30-42): Net losses resulting from the loss of IP. It is calculated by subtracting the property loss forecast from the base forecast.

National Impacts (lines 44-53): This section presents the impacts of the IP Theft affecting the nation as a whole.

Trade (line 46): The net trade balance will decrease because of a reduction in U.S. exports, plus an increase in U.S. imports resulting from the IP Theft. The reduction in exports is calculated by taking the net change in foreign sales (line 31) minus initial contract sales (line 33). The increase in imports is shown as civilian losses in line 38.

Royalties (line 47): The loss in royalties as a result of the foreign licensee not winning the contract. Note that the loss in D55 ($1 million) represents the loss of a license fee that would have been awarded to the U.S. firm had the licensee won the contract. Profit from parts sales tied to the licensing agreement are also included.

Taxes (payroll) (line 48): The loss of payroll taxes resulting from fewer employees earning wages to pay taxes.

Taxes (corporate) (line 49): The loss of corporate income tax resulting from the company and its suppliers earning less revenue and less profits.

Total jobs (line 50): The number of jobs lost throughout the United States as a result of IP theft. This job total includes company, supplier, and indirect jobs. Jobs are represented in person years.

Company jobs (51): The number of jobs lost by the company as a result of IP theft. Jobs are represented in person years.

Supplier jobs (line 52): The number of jobs lost by the company's suppliers as a result of IP Theft. Jobs are represented in person years.

Indirect jobs (line 53): The loss of indirect jobs lost as a result of jobs lost by the U.S. firm's suppliers.

Company Impacts (lines 55-63): This section presents the financial impacts of IP theft affecting the company.

Revenue (line 57): The loss of company revenue resulting from reduced sales because of the IP theft.

Royalties (line 59): There are no loss in royalties under the post-bid scenario.

Profits (sales) (line 60): The profits resulting from sales are calculated by multiplying the total number of lost sales (line 41) by the standard profit made on each unit ($7,478).

Profits (margin) (line 61): The loss in profits due to a squeeze on the company's profit margin because of increased competition. Margins are squeezed either through lower sales prices, and/or through higher per unit costs as the number of units produced per day declines.

Taxes (line 62): The company's taxes will actually decrease as a result of reduced revenues and profits. This is represented as a gain to the company, which partly offsets the loss in profits.

Supplier Impacts (lines 66-72): This section presents the financial impacts affecting the company's suppliers.

Revenue (line 68): The loss of suppliers' revenue resulting from reduced sales because of the IP theft.

Profits (line 69): The loss of profits resulting from a loss of sales. Calculated by multiplying supplier revenue by a 12.5% average supplier profit rate.

Taxes (line 70): The suppliers' taxes will actually decrease as a result of reduced revenues and profits. This is represented as a gain to the suppliers, which partly offsets the losses in profits.

PREPARED STATEMENT OF NEIL J. GALLAGHER, DEPUTY ASSISTANT DIRECTOR, CRIMINAL DIVISION, FEDERAL BUREAU OF INVESTIGATION

Good morning Chairman Saxton, Vice Chairman Mack, and Members of the Committee. I welcome this opportunity to provide insight into the Federal Bureau of Investigation's effort in the fight of economic crimes to include transnational crime.

Economic crimes affect a wide variety of industries, businesses and citizens. The theft of trade secrets has caused billions of dollars in losses and created a vulnerability within all types of industry. The significant and most positive advances in technology have also allowed businesses and financial institutions to become prey of a new age of criminals. The World-Wide Web has allowed for an endless barrage of frauds, scams, intrusions, and piracy. Cyberbanking has added a new dimension of potential financial institution fraud. In this computer age where network communication has become borderless, what the FBI has traditionally worked as an economic crime has the potential of becoming a transnational crime within a matter of seconds.

The FBI's task in fighting economic crime has dramatically changed with advancements in technology. New methods of economic crimes are being addressed with the assistance of new laws passed by Congress such as the Economic Espionage Act of 1996 (EEA) and the No Electronic Theft Act. At the same time, there is an increased emphasis on the training of FBI agents and providing them with the tools necessary to investigate these often complicated cases.

According to a study reported in 1996 by the American Society for Industrial Security regarding intellectual property loss, potential known losses to all American industry could amount to as much as $63 billion, with current losses occurring at a rate of $2 billion a month. The high-tech industry has an average loss per incident reported of $19 million. The specific portion of this attributable to domestic companies stealing trade secrets from one another cannot be determined with certainty. However, as we move further and further into the information age, the value and accessibility of various forms of intellectual property continues to increase. As this information becomes easier to access and/or steal, and its value continues to increase, the frequency of its theft is certain to increase as well.

In the increasingly competitive area of high technology, theft by rival companies of one anothers new products/trade secrets is inevitable and burgeoning. In much the same way we used to have to deal with employees embezzling funds from their employer; we are now dealing more and more with employees stealing trade secrets from their employers and attempting to sell them to the competition.

The Economic Espionage Act of 1996, signed into law by President Clinton on October 11, 1996, provided law enforcement with a tool to deal more effectively with trade secret theft. The Economic Espionage Act has helped to protect valuable U.S. trade secrets. The statute was the result of a Congressional mandate to provide law enforcement with a tool to deal effectively with trade secret theft. The law penalizes commercial theft of trade secrets in cases not involving foreign powers under the newly created statute Title 18, U.S.C. Section 1832. Prior to this law being enacted, the FBI had to rely on general statutes such as "Interstate Theft of Stolen Property" and "Fraud by Wire" to prosecute thefts of high-tech secrets. These statutes were often difficult to apply due to the lack of an interstate nexus.

These difficulties become more complex when applied to transnational crimes.

The Federal Bureau of Investigation took advantage of this law as soon as it was passed, receiving an arrest and conviction within two months of the enactment of the law. On December 7, 1996, 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 Pittsburgh Plate Glass information for $1,000 to a Pittsburgh agent posing as a representative of Owens-Corning, Toledo, Ohio. Both subjects were charged under Title 18, U.S.C. Section 1832. Patrick Worthing was sentenced to 15 months in jail and three years probation for the Theft of Trade Secrets.

Following the passage of the EEA, the FBI made an effort to educate agents in all 56 field offices regarding the elements of this new law. Six regional conferences sponsored by FBI Headquarters were held in the summer of 1997, with participation from all the field offices. Several of the conferences also allowed participation of industries in the area. Management and security personnel from these companies were given information regarding the new law and how best to protect their trade secrets. This coming together of FBI and private industry is critical

to our success in battling economic crime. It allows for increased communications and cooperation with private industry. At the same time, it provides for a unique opportunity for the FBI investigators to better understand the complexities and sensitivities of the industry from experts within that industry. These regional sessions have increased the number of agent personnel having the special training required to address the often sensitive needs of the high-tech industry.

The number of theft of trade secret investigations has continued to increase. In October of 1997 there were fifteen pending investigations. Currently there are 37 pending theft of trade secret investigations. These include investigations in Silicon Valley in California dealing with high tech industries to cases in locations such as Missouri and Tennessee. This increase in pending investigations is due in part by the positive relationships that the FBI has developed with industry and the resulting increased awareness of this growing crime problem.

The FBI is working to identify cities that are centers for high-tech industries. These cities will be afforded the training necessary to identify and investigate theft of trade secret and Intellectual Property Rights infringement matters. High-tech task forces will be encouraged to better utilize resources to address this crime problem.

Examples of recent cases charged under Title 18, U.S.C. Section 1832:

- Memphis: On October 3, 1997, the Memphis Division of the FBI arrested Steven Louis Davis, who was indicted in the Middle District of Tennessee on five counts of fraud by wire and theft of trade secrets. Wright Industries, the victim company and a sub-contractor of Gillette, had fully cooperated with the FBI's investigation. Although the FBI knows that Davis reached out to one foreign owned company (BIC), it is unclear if he was successful in disseminating trade secrets overseas. The FBI, however, has learned that a competitor in Sweden had seen the drawings of the new Gillette razor. Davis pled guilty on 1/23/98. Potential loss prevented was in the hundreds of millions of dollars.
- Cleveland: On September 5, 1997, Pin Yen Yang, and his daughter Hwei Chen Yang (aka Sally Yang) were arrested on several charges, including Title 18, U.S.C. Section 1832. Also charged is the Four Pillars Company, which has offices in Taiwan, and a registered agent in El Campo, Texas. It is alleged that the Four Pillars

Company, Pin Yen Yang, Sally Yang, and Dr. Ten Hong Lee were involved in a conspiracy to illegally transfer sensitive, valuable trade secrets and other proprietary information from the Avery Dennison Corporation, Pasadena, California, to Four Pillars in Taiwan. Dr. Lee has been an Avery Dennison employee since 1986, at the company's Concord, Ohio facility. Dr. Lee allegedly received between $150,000 and $160,000 from Four Pillars/Pin Yen Yang for his involvement in the illegal transfer of Avery Dennison's proprietary manufacturing information and research data over a period of approximately eight years. Direct development costs of technology transferred during this time is estimated to be in the tens of millions of dollars. On October 1, 1997, a Federal Grand Jury returned a 21 count indictment, charging Four Pillars, Pin Yen, and Sally Yang with attempted theft of trade secrets, mail fraud, wire fraud, money laundering, and receipt of stolen property. On the same date, Dr. Ten Hong Lee pled guilty to one count of wire fraud.

At the same time, we must recognize that technological advances are making corporate spying and theft easier and cheaper. Industrial espionage is most often carried out to gain access to corporate strategic plans, research and development information, and manufacturing process data. The power of computer technology has increased means for the theft and transfer of trade secret information. Computer age communications connectivity, commercial enterprise activities, and the posting and accessibility of corporate data on office workstations and home personal computers have made it extremely easy to copy and steal valuable trade secret information. This information can potentially be transferred transnationally as easily as it can be transferred across town.

Public and private sector organizations that rely on information technologies are diverse. Within the government, information technologies provide leverage for performing traditional missions more efficiently, e.g., law enforcement, intelligence gathering and exploitation, and national defense. In the private sector information systems allow rapid, efficient transfers of information and capital, enable a new wave of electronic commerce, and enable far-flung, technically complex operations to exist over vast geographic distances.

However, as commercial information technologies create advantages, their increasingly indispensable nature transforms them into high-value targets. Moreover, in practice these developments have

resulted in diminished systems redundancy and the consolidation of core assets, heightening the risk of catastrophic single-point failures.

Disgruntled employees, disaffected individuals or groups, organized crime, domestic and international terrorists, and adversary nations are all potential sources of attack.

Terrorists, transnational criminals, and intelligence services are quickly becoming aware of and exploiting the power of information tools and weapons. This has been true in the past as new means of communication, transportation, and secrecy have been introduced to the public. For example, narcotic traffickers began using communications advances such as pagers and cellular phones soon after their introduction to the public.

In yet another area, cyber banking is redefining consumer banking and creating new opportunities for high-tech financial institution crime. A recent Internet survey indicated that electronic banking is anticipated to increase 600% in the next two years. In the latter part of 1997, the Federal Deposit Insurance Corporation (FDIC) estimated that over 1,100 banks and thrifts are maintaining a presence on the World-Wide Web. Although many sites are primarily established for advertising, a growing number are beginning to offer transactional capabilities, including funds transfers.

The use of electronic access products to infiltrate banking systems have occurred, and with the use of the Internet, can occur from halfway around the world. One computer intrusion investigation involving the compromise of a major U.S. financial institution's cash management system resulted in the convictions of all seven foreign nationals involved. Potential losses of $10.4 million involving attempted fraudulent wire transfers were limited to $400,000 as a result of the FBI's lead in an international effort to identify the source of the intrusion and the individuals responsible. As global interconnectivity, access to the Internet, and electronic commerce increases, the threat of electronic exploitation will expand exponentially.

In response to this threat, the FBI, in cooperation with Department of Justice, Department of Treasury and representatives of financial regulatory agencies, has launched a cyberbanking initiative to examine the risks and potential losses associated with electronic banking technology. A working group has been established to focus on current and potential criminal activity in the emerging field of cyberbanking. The primary function of this working group is to insure that all

government agencies involved with the operation or regulation of cyberbanking are aware of the potential for fraud in any electronic banking scheme developed for use by the public. A secondary function is to insure that, in the development of cyberbanking systems, adequate fraud prevention measures are implemented so that frauds against the system can be detected, investigated, and prosecuted.

Coprehensive crime statistics involving electronic money and computer fraud and abuse are difficult to obtain. The FBI is working closely with federal banking regulators and the financial institution industry to evaluate methods by which computer related activity can be statistically tracked and monitored in order to assure that fraudulent activity of this nature is reported. The Suspicious Activity Reporting System (SAR), currently used by financial institutions to report fraudulent activity could be used, with some minor modification, to provide a simple and straightforward means for victims to report this increasing crime problem. The FBI and federal bank regulators have already worked together to produce guidance to the financial industry for reporting of computer crimes on SARs.

Case examples of cyberbanking fraud:

- In 1994, subjects in Russia gained unauthorized access to Citibank's Cash Management System. As a result, more than $10 million was wire transferred to preestablished accounts throughout the world. It was unclear where the attack was originating when the FBI began to monitor the cash movements through Citibank's central wire transfer department. Monitoring began in July and continued into October, during which there were 40 transactions. Cash was moved from accounts as far away as Argentina and Indonesia to bank accounts in San Francisco, Finland, Russia, Switzerland, Germany and Israel. In the end, all but $400,000 taken before monitoring began was recovered. The investigation resulted in six foreign nationals being charged in the United States. Citibank says it has found no evidence of insider cooperation with the hacker. Vladimir Levin was arrested in February 1995 by Scotland Yard based upon a provisional warrant and was extradited from England in September of 1997. He pled guilty on January 23, 1998 to conspiracy.
- In April of 1997, telephone calls were made to banks in Portland, Oregon and Boston, Massachusetts claiming that the institutions, and 49 other financial institutions, had been targeted by an

environmental group. The caller explained that the group had penetrated the bank's computer systems and if the banks did not make $2,000,000 "donations" to the group, the computer systems would be brought "to a screeching" halt. The caller further explained that timing devised had been utilized and if the $2 million dollar donations were not received by the group, the computer systems would crash within the next week. He also warned that if the banks involved law enforcement in the matter, the systems would be destroyed immediately. The caller advised his group had previously penetrated computer systems within the Central Intelligence Agency and other unnamed federal agencies. A subsequent telephone call was traced to a public pay phone and the subject was arrested. The subject pled guilty to one count of Title 18, U.S. C. Section 875 (Interstate Extortion) and was sentenced to six months in jail followed by three years supervised release.

The Financial Times reported in an article in August 1996 that the market for Internet banking is poised to grow sharply in the next three years, affecting the competitive advantage enjoyed by traditional banks as demand for Internet banking services takes off. It noted a survey of Internet banking by an international management consultant, which found that 154 European banks already have sites on the World-Wide Web, with sites increasing at a rate of nearly 90 percent a year.

The article went on to state that the cost of Internet banking run at on 15-20 percent of income, compared with an average cost:income ratio for the banking industry of about 60 percent. Starting an Internet bank from scratch costs about $1 million - one can buy all the software off the shelf. But a well established bank has to integrate it with their existing systems dramatically adding to the cost of setting up an Internet bank. Internet banking has the potential of changing the type of financial industry law enforcement will have to work with in combating financial crimes. The banks from other countries that are on the Internet can potentially provide other avenues for subjects for money laundering, wire transfers, and hiding of assets.

There have been reported incidents of bogus investment banks appearing on the Internet. These banks solicit money for investment and account creation. In reality, these banks do not exist and disappear as quickly as they appear. One such Internet bank was the subject of an Office of the Comptroller of the Currency (OCC) special alert. The Freedom Star National Bank of Arizona began soliciting deposits on the

Internet and offering high interest rates. The entity had not been granted a national bank charter by the OCC nor were its deposits insured by the Federal Deposit Insurance Corporation. This activity was stopped by the OCC special alert. Banking regulators are in the process of analyzing these type of fraudulent banks for criminal referral to the FBI.

The use of the Internet to market fraudulent investment schemes is becoming epidemic. An example of this type of scheme involves a multilevel operation doing business under the name Netware International, believed to had approximately 2,500 members throughout the United States. Netware provides false, fraudulent and misleading representations in order to solicit funds from new and existing members. Promotional information distributed over the Internet indicated that Netware was forming a private bank with full services and deposits insured by the National Union Fire Insurance Company of Pittsburgh, Pennsylvania. The information also indicated that the bank was expected to earn a profit of 25 percent per year, and that the members who sell two or more memberships would share in the profits of the bank. National Union Fire Insurance Company denied any affiliation with Netware. Nearly $1 million has been seized to date in this investigation. The investigation into Netware continues.

Internet banking is but one of many Internet frauds that the FBI is addressing. The types of frauds are numerous and have been found to often have international connections. The National Consumers League has stated that they receive more than 100 scam complaints each month. They range in size from $10 to $10,000. The ten most frequent fraud reports involve undelivered Internet and online services; damaged , defective, misrepresented or undelivered merchandise; auction sales; pyramid schemes and multilevel marketing; misrepresented cyberspace business opportunities and franchises; work-at-home schemes; prizes and sweepstakes; credit card offers; books and other self-help guides; and magazine subscriptions.

Banking and investment industries have not been the only industries dramatically affected by Internet fraud. The copyright industry has lost millions of dollars due to piracy of software, music and interactive digital software on the Internet. Hundreds of digital jukeboxes are surfacing on the Internet. The digital jukeboxes release music over the Internet in the form of MPEG3 digitally compressed files, called MP3s, which can be downloaded free of charge on to home computers. Most pirate jukeboxes are run for free by young music buffs, often students using university

servers. Downloading music free of charge from the Internet is becoming increasingly popular among the 15 to 30 year olds who tend to be frequent record buyers and are often computer enthusiasts. The music industry now stands to lose substantial sums of money because of the unauthorized distribution of its copyrights.

Bulletin Board Services (BBSs) have long been a potential source of computer software and interactive digital software piracy. There exist BBSs whose only function is engaging in criminal activity. These BBSs provide a listing of software programs available for downloading through the Internet. The actual cost of the software involved is negated through a bartering system. The use of this bartering type system has been very effective in circumventing the law until recently. The No Electronic Theft Act, passed by Congress and signed by the President on December 17, 1997, makes it a crime to possess or distribute multiple copies of on-line copyrighted material, for profit or not. This has eliminated the ability to circumvent the law by not exchanging money.

On 1/28/97, the FBI in San Francisco executed eight search warrants simultaneously in six states in connection with an undercover investigation, code name Cyber Strike. Cyber Strike has focused on increasingly organized efforts by individuals and groups to conduct the piracy of computer software produced by some of the nation's largest software firms. Seizure of more than seven Gigabytes of illegal transactions (equivalent to 20 million pages of information) was made. Following the search, eight BBS systems were dismantled and their equipment seized. The searches were conducted in Atlanta, Georgia; Columbus, Ohio; Miami, Florida; Oklahoma City, Oklahoma; Des Moines, Iowa; Pittsburgh, Pennsylvania; San Leandro and Cedar Ridge, California.

Traditional crimes have taken on a new appearance over the Internet. An example of this is Internet sports gambling. Earlier this month the New York FBI field office filed complaints against fourteen managers and owners of six Internet sports betting companies that operated offshore and allowed bettors in the United States to gamble on football, basketball, and other sports. Attorney General Janet Reno said in a statement: "The Internet is not an electronic sanctuary for illegal betting. If a state outlaws soliciting or accepting bets, you can't evade those requirements by going on line." This is an example of how the FBI is constantly working to keep abreast of new crime schemes and is

focusing our investigative resources to address these emerging crime problems.

Software piracy, as well as all other types of piracy, continues to be an international concern. According to the International Intellectual Property Alliance, copyright piracy cost an estimated loss of $10.8 billion to U.S. copyright industries. In addition, the International Anti-Counterfeiting Coalition has estimated that the cost due to trademark infringement in the world to be $250-350 billion. U.S. industries represent the leading edge of the world's high technology, entertainment and apparel industries. Piracy of copyrighted and trademarked items cost the U.S. economy tax revenue and jobs because of the manufacture, distribution and sale of counterfeit goods.

The FBI has supported training in intellectual property rights issues in a number of foreign countries to include Russia, China, Egypt, Peru, and Latvia. Piracy is more than a domestic crime problem. It is an international crime problem that involves organized groups that conduct their counterfeiting enterprises multi-nationally. Through the FBI's efforts in international training and established contacts with foreign law enforcement officials throughout the world, the groundwork has been laid for an international effort in addressing this international crime problem.

To conclude, a major concern now facing law enforcement is how rapidly the threats from criminals, both domestic and international, are changing, particularly in terms of technology. The challenge to law enforcement is our ability to keep pace with these criminals who pose a threat against United States, our citizens, and our industry. The FBI is working closely with law enforcement officials in other countries to combat computer crimes and enhance coordination, and improve our combined capabilities. Cooperative efforts with industry have also been intensified to facilitate the prevention and detection of emerging cyber crimes. The types of economic crimes described today can and do have a lasting effect on our nation's economy. The FBI is aggressively investigating these types of economic crimes. Chairman Saxton, I wish to thank you and the members of the Joint Economic Committee for your support. I applaud your commitment and confidence in this important area of the FBI's responsibility.

PREPARED STATEMENT OF MICHAEL A. VATIS, DEPUTY ASSISTANT DIRECTOR AND CHIEF, NATIONAL INFRASTRUCTURE PROTECTION CENTER, FEDERAL BUREAU OF INVESTIGATION

Chairman Saxton, Vice Chairman Mack, and Members of the Joint Economic Committee: Thank you for this opportunity to discuss cybercrime, the vulnerabilities of our Nation's critical infrastructures to increasing cyber threats, and what the Federal Bureau of Investigation (FBI) is doing to combat these problems.

As we continue to rush into the Information Age, our society is moving increasingly on-line. We use computers, the Internet, and other new "information technologies" to conduct business, perform scientific research, engage in personal communications, and do just about anything else that inventive minds can think of. But as society as a whole is moving on-line, so are criminals. Criminals use computers to facilitate crimes committed in the physical world. For example, they can use computers and the Internet to communicate with co-conspirators or to keep accounts of their illicit gains. Criminals also use these tools to engage in criminal activity on-line. For example, they use the Internet to defraud unsuspecting senior citizens, disseminate child pornography, steal credit card numbers, and rob banks by electronically shifting funds to their own off-shore accounts.

But the Internet and other advances in information technology do not merely give criminals new means to commit traditional crimes like theft or fraud. They also allow criminals and other malicious actors to cause new types of harm that go well beyond the potential loss to the individual victim and can affect our national economy and, indeed, our national security.

What type of harm am I talking about? The everyday functioning of our economy depends on the delivery of certain critical services. While we once got along fine without electrical power, think of the consequences if the power went out for a week – not just in one town or city, but across the whole Eastern Seaboard. And while plenty of people made their fortunes before the telephone, imagine what would happen to the Fortune 500 if they were deprived of telephone service for a few days.

There are several services whose availability we may take for granted, but which are truly critical to the smooth functioning of our society. We call these vital services our "critical infrastructures." Executive Order 13010, signed in 1996, lists the following eight

infrastructures as "critical" to our economic health and our national security: telecommunications, banking and finance, transportation (including roads, railroads, airplanes and airports, mass transit, ports and harbors), electrical energy, gas and oil supply, water supply, emergency services (fire, health, police), and government operations. These infrastructures are defined as "critical" because their debilitation or destruction would have a significant adverse impact on our national economy or national security.

In the United States, we are able to expect things to work because our infrastructures are highly developed and efficient. Individuals and families can wake up in the morning confident that the lights will work, water will flow from the tap, and the trains will run. Businesses, too, can plan their activities and investments around the certainty that they will have ready access to telecommunications, that gas or oil will supply power to their factories, that their goods will be transported by truck, rail or airplane, and that funds can be safely deposited or withdrawn from their bank accounts. It is a given, in both our personal and professional lives, that essential goods and services will be available when needed.

Not so long ago, our dependence on these infrastructures did not pose a significant problem because there was little risk that these vital services would be knocked out. Only a rare and isolated occurrence, such as an earthquake or tornado or an accidental power outage could knock out a critical service over a broad area. The physical breadth of the infrastructures made it difficult for a potential malefactor to cause anything other than an isolated disturbance. And physical security measures adopted to prevent theft or vandalism generally also kept out those who would seek to destroy an infrastructure's ability to continue operating. A strong fence and a good security staff fended off not only thieves and vandals, but also terrorists. Moreover, our geographic isolation from other countries made it difficult for foreign adversaries to launch an attack on our infrastructures.

The Information Age, however, has changed things dramatically. For while information technologies create dramatic increases in efficiency and productivity, our dependence on them creates new vulnerabilities.

All critical infrastructures now rely on computers, advanced telecommunications, and, to an ever increasing degree, the Internet, for the control and management of their own systems, for their interaction with other infrastructures, and for communications with their suppliers

and their customer base. For example, electric power grids and natural gas pipelines are controlled by computer systems, and those computers may be linked to each other and to the company headquarters by publicly-accessible telecommunications systems and commercially available information technologies to allow efficient management of power generation and smooth delivery to consumers. Billions of shares are traded each day over the telephone or Internet, and the stock exchanges could not function today without their vast networks of computers. Banks no longer rely on ledger books and safe deposit boxes to account for and secure their holdings, but depend on computerized accounting systems to manage depositors' accounts. The telecommunications system itself no longer uses operators to manually plug in calls to a switchboard but depends on computerized switching stations to handle the billions of calls placed each day. The government also relies on computers and publicly available communications systems to conduct the nation's business. Public and private networks and databases use the same technology, and vulnerabilities that affect one also affect the other.

But this reliance on new technologies comes with a price, and that price is a new vulnerability to those who would cause harm. For just as the new technologies make it easier for companies to communicate and control their businesses, they also make it easier for malicious actors to cause harm. The new vulnerability stems in part from the fact that the Internet and modern telecommunications systems are inherently open and accessible. That means that, with a certain amount of technical skill, one can use these communications media to get inside a company's or a government agency's computer system without ever physically penetrating its four walls. Moreover, the increased centralization of command and control systems afforded by the new technologies also means that, once inside that system, a potential malefactor can use those same technologies to cause harm over a much broader area than he ever could have hoped using physical weapons such as a bomb.

This vulnerability is exacerbated by several factors. First, most of our infrastructures rely on commercially available, off-the-shelf technology. This means that a vulnerability in hardware or software is not limited to one company, but is likely to be widespread, affecting every entity that uses the same equipment. A malefactor with knowledge of this one vulnerability can therefore attack multiple victims across the country, with just a few strokes on a keyboard.

Second, our infrastructures are increasingly interdependent and interconnected with one another. For example, the banking system depends on the availability and reliability of the telecommunications system and the Internet, which in turn rely on electrical power. Our transportation system depends on the availability of gas and oil supplies, which in turn are controlled through the use of new information technologies. The infrastructures are thus increasingly interdependent, so much so that it is difficult to predict the cascading effects that the disruption of one infrastructure would have on others.

Third, our telecommunications infrastructure is now truly global. Satellite communications, the Internet, and foreign ownership of telecommunications carriers in the U.S. have all combined to undermine the notion of a "National" Information Infrastructure. This means that our geographic isolation no longer acts as a moat to fend off foreign adversaries. Instead, it is now as easy to break into an infrastructure's network from St. Petersburg, Russia, as St. Petersburg, Florida. A personal computer and a telephone connection to an Internet Service Provider anywhere in the world are enough to conduct an attack.

Software is one weapon of cyber attacks. Such software includes, among others, computer viruses, Trojan Horses, worms, logic bombs, and eavesdropping "sniffers" that can be used to obtain passwords that allow hackers "root access" control of a computer system. Advanced electronic hardware also can be used in cyber attacks, including such items as high-energy radio frequency (RF) weapons, electromagnetic pulse weapons, RF jamming equipment, or RF interception equipment. These weapons can be used to destroy property and data; intercept communications or modify traffic; degrade the integrity of data, communications, or navigation systems; and deny crucial services to users of information and telecommunications systems.

So that's the vulnerability picture in the cyber world. But what about the corresponding threat? In the physical world, the range of people or groups that would have the means and motive to cause widespread destruction of an infrastructure are relatively limited – terrorist groups and hostile nations are the most likely actors. But the accessibility of the information infrastructure, global connectivity, and the rapid growth of a computer-literate population combine to ensure that millions of people around the world possess the means to engage in a cyber attack. The spectrum of threats in this new cyber world is staggeringly broad and varied, including: the disgruntled insider seeking

revenge against his employer; the recreational hacker out to test his "cracking" skills; organized crime groups seeking illicit financial gain; domestic or international terrorist groups bent on causing harm to send a political message; foreign intelligence services seeking companies' proprietary data or sensitive government information; and hostile nation states utilizing information warfare as part, or instead, of a strategic military attack. Let me discuss each of these threats in a little more detail.

Perhaps the most imminent threat today comes from insiders. Insiders have the advantage of not needing to break into computer systems from the outside, but only to use, or abuse, their legitimate access. Many of the computer intrusion reports the FBI and other law enforcement organizations receive have at their core an employee, former employee, consultant, or temporary employee who has exceeded his or her access, often in revenge for some perceived wrong. These individuals often have intimate knowledge of where the most sensitive information is stored, how to access the information, and how to steal or damage the data.

Recreational hackers are also increasingly dangerous, in part because of the widespread availability of "cracking" tools on hacker websites. One no longer needs to have a sophisticated understanding of computers and the Internet to successfully crack into a company's systems. Rather, one needs only to download an automated hacking tool from a website, compile the source code using a program readily available on the Internet, and click on a button to launch an attack on any number of target sites.

Moreover, the problem is exacerbated by our continued romanticization of hackers as technical whizzes who are not really doing anything wrong but are actually providing a service by pointing out the vulnerabilities in an individual's or a company's or government agency's system. But do we praise the burglar for demonstrating the vulnerability of our home security by breaking in and stealing our cash or jewelry? Even if he does not steal or break anything, the simple invasion of our private property causes a feeling of violation and vulnerability that would send chills down all our spines. Or do we thank the vandal who breaks into the corner store and defaces or destroys someone else's property? Of course not. But, similarly, we should not tolerate or condone analogous acts committed with computers. These are not acts that occur in some ethereal "cyberspace" that is somehow divorced from

the real world. These are acts that are very real, and can cause serious harm. It is no joke when an individual's private E-mail communications are intercepted, or when a company's proprietary data is stolen or destroyed, or when a government agency's sensitive data is compromised. And these acts can have serious physical consequences. No one would laugh if a hacker caused air traffic control to go down at an airport, as happened in a case in Massachusetts that recently resulted in a plea bargain. Or if a hacker tied up 911 emergency phone services, potentially denying critical aid to people with true emergencies, as happened in a recent case in Florida. Our society has to do a better job of educating our children and young adults that breaking into someone else's computer system has serious real-world consequences, and is a serious crime.

Where hackers formerly may have been motivated by the technical challenge of breaking into a computer system, the motivation may now be shifting more toward hacking for profit. As more and more money is transferred through computer systems, as more fee-based computer services are introduced, and as more sensitive proprietary economic and commercial information is stored and exchanged electronically, we will see criminal hackers use their computer skills for illicit gain.

Terrorists and transnational criminals also rapidly are becoming aware of and exploiting the power of cyber tools. This has been true in the past as new means of communication and secrecy have been introduced to the public. For example, narcotics traffickers began using communications advances such as pagers, cellular phones, and unbreakable encryption soon after their introduction to the public. The fantastic growth of the Internet and other global information networks grants increasing numbers of users with hostile intentions access to global networks – and to those United States networks upon which critical infrastructures depend.

Finally, as our nation's defense and intelligence agencies increasingly rely on commercially available information technologies and publicly accessible communications systems for their everyday work, foreign intelligence services and hostile nation states will increasingly seek to acquire and use cyber tools to conduct espionage or engage in "information warfare" against us. Several different commissions, including the President's Commission on Critical Infrastructure Protection and the National Defense Panel, have recognized that no nation or group hostile to the United States can match us in traditional military firepower. Because of this, they would not be expected to take

us on in a frontal or "symmetrical" attack. Rather, they would utilize irregular, "asymmetrical" attacks that hit us where we are most vulnerable. And one of those vulnerabilities is our reliance on information technologies for command and control of our national security activities as well as for the daily functioning of our privately-owned critical infrastructures. This vulnerability is particularly attractive to foreign enemies in that it is just as easy to crash a system from a computer terminal overseas as it is from one in the United States.

Some would say that this vulnerability is overstated, that there are sufficient technological security tools to protect against malicious hackers and crackers, and that infrastructures have built in redundancies to their systems to prevent catastrophic system failures in the event of a successful intrusion. I'm afraid that the facts prove otherwise. Although we have not experienced the electronic equivalent of a Pearl Harbor or Oklahoma City as some have foretold, the statistics and our cases demonstrate our dangerous vulnerabilities to cyber attacks.

A 1998 study by the Computer Security Institute shows that 64% of companies polled reported information system security breaches – an increase of 16% over last year. The total financial losses from the 241 organizations that could put a dollar figure on them adds up to $136,822,000. This figure represents a 36% increase in reported losses over the 1997 figure of $100,115,555 in losses.

While the Carnegie Melon CERT/Coordination Center reported a small reduction in security incidents (2,134 in 1997, down from 2,573 in 1996), the type and scope of attacks indicates a disturbing increase in the use of automated scripts, enabling malevolent network users to attack very large numbers of systems with much greater efficiency.

A study of 300 Australian companies by Deloitte Touche Tohmatsu found that over 37 percent of the companies experienced some form of security compromise in 1997, with the highest percentage of intrusions (57%) occurring in the banking and finance industry.

A 1996 survey by the American Bar Association of 1,000 companies showed that 48 percent had experienced computer fraud in the last five years. Company losses were reported to have ranged from $2-10 million.

In 1996 the Defense Information Systems Agency (DISA) estimated that as many as 250,000 attacks on DOD systems may have occurred in 1995. DISA indicates that the number of attacks has been increasing each year for the past few years, and that trend is expected to continue.

Finally, we at the FBI have seen significant increase in the number of pending computer intrusion investigations and in the number of successful prosecutions. Pending cases have increased 133% from the beginning of FY 1997, from 206 to 480. In FY 1997, there was a 110% increase in informations and indictments (from 10 to 21), a 950% increase in arrests (from 4 to 42), and an 88% increase in convictions (from 16 to 30).

As a caveat, let me state that it is not clear what accounts for these increases in our own case statistics or in the numbers reported by the private studies. It may be that systems administrators have simply gotten better at detecting intrusions, or that companies have become more willing to share information about their own exploited vulnerabilities. Or, it may be that the number of intrusions has risen significantly. Most likely, in my view, all three things are occurring. Regardless of the cause, however, these numbers clearly indicate significant vulnerabilities to cyber attacks.

Let me now give you a few examples of the types of computer crimes we have seen in recent years to further illustrate the problem:

You are undoubtedly aware of the recent series of intrusions into Department of Defense and other government agency computers across the country. This case involved widespread illegal intrusions into government systems using holes in the systems' software. I cannot go into detail on this matter because it is a pending case, but the FBI recently identified two juveniles in California who appear to have been responsible for many of the intrusions. And the Israeli National Police, working with FBI, Air Force, and NASA investigators, this week placed under house arrest one individual who also appears responsible for many of the intrusions. While we are still determining the extent of harm caused by these intrusions, the potential harm was obviously enormous. Even the unclassified systems used by DoD and other government agencies contain an enormous amount of important and sensitive data, the loss or alteration of which would have serious adverse consequences for our national security.

Many of you have also probably read about the plea bargain in Massachusetts this week of a teenage hacker who was able to break into the former NYNEX (now Bell Atlantic) system and, through it, disable telecommunications at a regional airport, cut off services to the airport's control tower, and prevent incoming planes from turning on the runway

lights. This case is a wake-up call for those who would argue that hacking is simply harmless fun.

In 1994, foreign crime groups operating in several different countries were able to hack into the Citibank Cash Management System, which is used for banking functions such as wire transfers. The criminals compromised passwords to impersonate account holders worldwide, and attempted 40 transfers totaling $10 million. As a result of early detection by Citibank officials, and close cooperation between Citibank investigators, payee banks, foreign police, and the FBI, the perpetrators were tracked down and arrested, and actual losses were limited to $400,000. But imagine if the hackers had been intent not simply on stealing funds, but on destroying Citibank's account records or denying service to Citibank customers. The effects in such a scenario would have had much more serious and widespread consequences.

In another case, hackers from Germany recently captured the customer credit card files of a Miami company. The hackers threatened to distribute all the credit card numbers unless they were paid ransom. When one of the hackers tried to pick up the money, he was arrested by German authorities. If the hackers had chosen to use the numbers instead of trying extortion, law enforcement may not have been able to stop them before they had caused significant financial loss.

An international computer hacker organization headquartered in Dallas, Texas successfully penetrated the networks of several telecommunications providers and acquired unlisted telephone numbers, personal addresses, credit information, and National Crime Information Center data, causing losses in excess of $500,000. The hackers installed a sniffer which compromised at least 15 telephone company systems including records, maintenance, and operational control system, and also illegally wiretapped the phone lines. The advanced level of expertise of the hackers was comparable to telephone company experts, and suggests that they could have disrupted telecommunications on a national basis if they had wanted to.

In July, 1997, the owner of a computer communications company sent, or caused to be sent, malicious computer code which resulted in the redirection of computer communications away from the computers of one of his competitors. This redirection of computer communications resulted in a direct loss to the victim company of at least $1,500,000. Additionally, millions of Internet users were denied access to various affected Internet sites.

These are just a few examples of the computer crime problem that we are seeing. But they illustrate the growing problem of cybercrime, the international dimension of the problem, and the increasing threat to our critical infrastructures. And, as I stated earlier, they demonstrate that this is not simply a problem of enforcing the law against imaginative criminals, but of protecting our economic health and national security.

Now let me tell you what the FBI is doing about it. On February 26 of this year, the FBI created the National Infrastructure Protection Center (NIPC). The NIPC's mission is to detect, deter, prevent, assess, warn, respond to, and investigate unlawful acts involving computer and information technologies and unlawful acts, both physical and cyber, that threaten or target our critical infrastructures. This means we do not simply investigate and respond to attacks after they occur, but we try to learn about them and prevent them beforehand. This requires the collection and analysis of information gathered from all available sources, and the dissemination of our analyses and of warnings of possible attacks to potential victims, whether in the government or private sector.

This broader mission also means that we in the FBI, and indeed law enforcement as a whole, cannot do this alone. Rather, this mission requires the combined efforts of many different agencies. The Defense Department has a critical role to play because its reliance on information technologies makes it a prime target for our adversaries and because it holds much of the government's expertise in defending against cyber attacks. Our intelligence agencies have an important role because of their responsibility for gathering information about threats from abroad. And other civilian agencies with jurisdiction over critical infrastructures, such as the Departments of Treasury, Energy, and Transportation, have similarly significant roles.

But this is also not just a role for the federal government. State governments must be involved because they own and operate some of the critical infrastructures and because their agencies are often the first responders in the event of a crisis.

And, perhaps most importantly, this mission requires the intensive involvement of the private sector. Private industry owns and operates most of the infrastructures, so it must be involved in helping us defend them. And it also has the greatest expertise in the technical problems and solutions.

In recognition of the vital roles all of these entities must play, the NIPC is founded on the notion of a partnership. It creates a partnership by including representatives from the other critical federal agencies, from state and local law enforcement, and from private industry. This will foster the sharing of information and expertise, and improve coordination among all the relevant actors in the event of a crisis. And it will augment the physical presence of these representatives by establishing electronic connectivity to the many different entities in government and industry who might have, and need, information about threats to our infrastructures.

Let me say at this point something about what we are not. We are not the Nation's super-systems administrator, responsible for physically securing everyone's systems against intruders or advising on the latest security software or patches to fix vulnerabilities. That role clearly must be filled by systems administrators in each company, by chief information officers in government agencies, and by industry groups and other entities with expertise in reducing vulnerabilities and restoring service. Rather, our role is to help prevent intrusions and attacks by gathering information about threats from sources that are uniquely available to the government (such as from law enforcement and intelligence sources), combining it with information voluntarily provided by the private sector or obtained from open sources, conducting analysis, and disseminating our analyses and warnings to all relevant consumers. And if an attack does occur, our role is to serve as the federal government's focal point for crisis response and investigation. That job is big and difficult enough, so I don't want to create any unwarranted expectations about what else we might do.

The NIPC incorporates and expands the mission and personnel of the FBI's former Computer Investigations and Infrastructure Threat Assessment Center (CITAC) which was created in 1996 to coordinate the FBI's investigations and response to the increasing problem of computer crime. The NIPC, located at FBI Headquarters in Washington, D.C., consists of three sections. The Computer Investigations and Operations Section (CIOS) is responsible for managing support to computer intrusion investigations conducted by our Field Offices, providing and coordinating technological support to all FBI investigations involving computers and information technologies, and for developing and managing an interagency Cyber Emergency Support Team (CEST) analogous to the Domestic Emergency Support Team and Foreign

Emergency Support Teams that are responsible for responding to terrorist acts in the U.S. or abroad. In addition, CIOS provides and coordinates subject matter experts, equipment, and technological support to cyber investigators from our Field Offices and other federal, state or local government agencies.

The Analysis and Warning Section (AWS) provides analytical support for computer investigations, and serves as the information clearing-house for research and analysis about physical and cyber threats and unlawful acts that target the critical infrastructures of the United States. It is charged with obtaining relevant information from all sources – law enforcement investigations, intelligence sources, open sources, and voluntarily provided industry data – analyzing it, and disseminating its analyses and tactical warnings to relevant consumers.

The Training, Administration, and Outreach Section (TAOS) has at its core the responsibility for coordinating the training and continuing education of cyber investigators in the FBI Field Offices, in other federal agencies, and in state and local law enforcement; and of personnel in the public and private sector involved in infrastructure protection. It also will direct our extensive outreach efforts to FBI Field Offices, other government agencies, industry, and academia, which are necessary to encourage the sharing of information about threats, vulnerabilities, and technological developments. In addition, the TAOS provides the administrative support that underlies and is necessary to all of the other activities of the Center.

Let me note, finally, that we have been in existence less than a month, so we are still very much in the early stages of building the Center. We have a lot of work to do in order to establish the necessary liaison with other agencies and the private sector, and to put in place our personnel and equipment. This will take time. But the Department of Justice and the FBI have taken an important first step in establishing this Center, in recognizing the need for an interagency and public-private partnership, and in realizing that the new challenges of the next century require new ways of thinking and creative solutions.

Thank you.

PREPARED STATEMENT OF LARRY E. TORRENCE, DEPUTY ASSISTANT DIRECTOR, NATIONAL SECURITY DIVISION, FEDERAL BUREAU OF INVESTIGATION

Good morning Mr. Chairman, Vice Chairman, and Members of the Committee. Thank you for this opportunity to join my colleague in providing the FBI's perspective in this area of growing concern.

As Mr. Gallagher has indicated, economic crimes have a serious impact on a wide variety of industries and businesses, and therefore upon the economic well-being of the United States. The ever increasing value of proprietary economic information in the global and domestic marketplaces, and the new uses for technology, have combined to enhance the opportunities and motives for conducting economic espionage.

Foreign governments and major foreign industrial sectors play a prominent role in their nation's business intelligence collection efforts. While a Cold War military rival stole military secrets about a state-of-the-art weapon or defense system, today's economic rival steals proprietary business information or government trade strategies. As a result, the intelligence agencies of some governments conduct economic espionage. These governments actively target U.S. persons, firms, industries and the U.S. Government itself, to steal our critical technologies, patented formulae, and business plans on behalf of their own economies.

Because trade secrets are an integral part of virtually every aspect of U.S. trade, commerce, and business, the security of trade secrets is essential to maintaining the health and competitiveness of critical segments of the U.S. economy.

In 1994, the FBI established an economic counterintelligence program as part of our national security strategy. The passage of the Economic Espionage Act of 1996 has greatly assisted the FBI in its battle against those who conduct economic espionage. The Act resolved many gaps in federal criminal laws. It fundamentally modernized our criminal code by protecting intellectual property through strong new criminal sanctions. Principally, The Economic Espionage Act created two new felony crimes. The first of the two crimes [Title 18, United States Code, Section 1831] punishes any person or company that steals trade secrets on behalf of a foreign government or entity. **Persons** convicted under this law face a maximum 15 year sentence and up to $500,000 fine. For organizations the fine can range up to $10,000,000.

The second crime, Section 1832, punishes the theft of trade secrets for simple **criminal gain** and does not require the intent to benefit a foreign entity. It carries a maximum 10 year jail term and up to a $500,000 fine for individuals and a $5,000,000 fine for organizations.

Under the law, a trade secret is defined broadly as any proprietary information that is reasonably protected from public disclosure and that derives independent economic value from being a secret for the rightful possessor. Importantly, the Economic Espionage Act has a provision protecting the victim's trade secret from public disclosure throughout the entire court process.

Prior to the passage of this Act, the FBI was already addressing hundreds of foreign counterintelligence investigative matters concerning hostile economic intelligence activities. That pace continues. The FBI has developed significant information on that foreign economic threat, to include: 1) identification of the foreign government sponsors of economic espionage; 2) the economic targets of their intelligence and criminal activities; and 3) the methods used to clandestinely and illicitly steal U.S. Government information, trades secrets and technology.

Additionally, the FBI has forged crucial partnerships with the Department of Defense, Department of Energy, and private industry to allow for prompt detection and successful investigative efforts in this area.

A number of countries continue to pursue economic collection programs. Foreign economic collection focuses on Science and Technology, as well as Research and Development. Of particular interest to foreign collectors are dual-use technologies and proprietary economic information which provide high profitability. Proprietary business information, i.e., bid, contract, customer and strategy information, is aggressively targeted. Foreign collectors have also shown interest in government and corporate financial and trade data.

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

An intelligence collector's best source continues to be a mole, or "trusted person," inside a company or organization, whom the collector can task to provide proprietary or classified information. Recently, we

have seen the international use of the Internet to contact and task insiders with access to corporate proprietary information. Other methodologies include the recruitment of foreign students, joint ventures, and the use of well-connected consultants to operate on behalf of a foreign government.

In conclusion, the National Security Division must continue to address the ever present threat to intellectual property, trade secrets and other proprietary economic information. The evolution of the global community and of technology itself presents a rapidly changing arena in which the foreign threat to U.S. trade secrets is constantly lurking. The FBI's efforts to build key relationships with other executive departments and with private industry will be crucial in the successful counterintelligence efforts focusing on the economic collection activities of foreign entities. Thank you for your time and your support of this critical area of concern to the national security of the United States.

O

ISBN 0-16-057323-8