FIGHTING CYBER CRIME

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

MAY 24, JUNE 12 AND JUNE 14, 2001

Serial No. 33

Printed for the use of the Committee on the Judiciary

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

U.S. GOVERNMENT PRINTING OFFICE

72–616 PS WASHINGTON : 2001

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

COMMITTEE ON THE JUDICIARY

F. JAMES SENSENBRENNER, JR., WISCONSIN, *Chairman*

HENRY J. HYDE, Illinois
GEORGE W. GEKAS, Pennsylvania
HOWARD COBLE, North Carolina
LAMAR SMITH, Texas
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
BOB BARR, Georgia
WILLIAM L. JENKINS, Tennessee
ASA HUTCHINSON, Arkansas
CHRIS CANNON, Utah
LINDSEY O. GRAHAM, South Carolina
SPENCER BACHUS, Alabama
JOE SCARBOROUGH, Florida
JOHN N. HOSTETTLER, Indiana
MARK GREEN, Wisconsin
RIC KELLER, Florida
DARRELL E. ISSA, California
MELISSA A. HART, Pennsylvania
JEFF FLAKE, Arizona

JOHN CONYERS, JR., Michigan
BARNEY FRANK, Massachusetts
HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
TAMMY BALDWIN, Wisconsin
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California

TODD R. SCHULTZ, *Chief of Staff*
PHILIP G. KIKO, *General Counsel*
JULIAN EPSTEIN, *Minority Chief Counsel and Staff Director*

SUBCOMMITTEE ON CRIME

LAMAR SMITH, Texas, *Chairman*

MARK GREEN, Wisconsin
HOWARD COBLE, North Carolina
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
BOB BARR, Georgia
ASA HUTCHINSON, Arkansas,
Vice Chair
RIC KELLER, Florida

ROBERT C. SCOTT, Virginia
SHEILA JACKSON LEE, Texas
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ADAM B. SCHIFF, California

JAY APPERSON, *Chief Counsel*
SEAN MCLAUGHLIN, *Counsel*
ELIZABETH SOKUL, *Counsel*
BOBBY VASSAR, *Minority Counsel*

CONTENTS

HEARING DATES

May 24, 2001

OPENING STATEMENT

WITNESSES

LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

June 12, 2001

OPENING STATEMENT

WITNESSES

FIGHTING CYBER CRIME: EFFORTS BY STATE AND LOCAL OFFICIALS

THURSDAY, MAY 24, 2001

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CRIME,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to call, at 1:42 a.m., in Room 2237, Rayburn House Office Building, Hon. Lamar Smith [Chairman of the Subcommittee] presiding.

Mr. SMITH. The Subcommittee will come to order. We welcome our witnesses today, and the audience as well, and I do want to explain why the hearing was delayed. It was through no fault of our own. Apparently there were three Subcommittees meeting this morning, and they decided to stagger them rather than have meetings conflict, and unfortunately we were scheduled, therefore, for 1:30 this afternoon. I know this may have inconvenienced our witnesses. I apologize for that, and hope you can still make your flights or get back home as you need to.

We are going to open the hearing today. I am going to have an opening statement. I will recognize other Members for their opening statements, and then we will get to our witnesses as quickly as possible.

States and localities have the primary responsibility of law enforcement in our Nation, so it is fitting to have State and local officials testify about their law enforcement efforts to reduce cyber crime. This is the Subcommittee on Crime's first of three hearings on the issue. The other two oversight hearings will focus on Federal efforts and businesses' concerns, and those two hearings will be later on in June.

As society has benefitted from cyber technology, so has criminal activity. Technology advanced and cyber crime followed. An article in the Washington Times today describes an Internet scheme that defrauded 56,000 people out of more than $117 million. Cyber crime takes many other forms, such as child pornography, piracy, fraud, computer security breaches, extortion, and e-commerce terrorism.

Terroristic threats to critical infrastructure present significant problems. Such an attack could have disastrous effects. For instance, a cyber crime attack on a utility company control center would cause power outages and halt critical services.

Cyber crime also threatens the safety and security of American children through the rapid spread of illegal child pornography on the web. Its proliferation is a growing public concern. According to

a recent poll, some 92 percent of Americans say they are concerned about child pornography on the Internet, and 50 percent of Americans cite child porn as the single most heinous crime that takes place online.

Unfortunately, laws defining cyber offenses and law enforcement technologies and training appear to lag behind technological advances and criminal activity. The Government Accounting Office recently reported that the lack of adequate information sharing and adequate staffing has hurt anti-cyber crime efforts. Better coordination and cooperation among Government agencies also is needed because cyber crime presents serious jurisdictional issues, some of which we will hear about in a few minutes from our witnesses.

Last week, while I was in Texas, I met with the Austin Police Department's high tech crime unit; the Texas Deputy Attorney General for Criminal Justice, who is here to testify today; and the Chief of the Texas Internet Bureau. All agree that cyber crime is a growing problem confronting States and localities, and that there needs to be enhanced coordination and cooperation at all levels of Government and with the private sector, as well.

Since technological advancement will continue to transform our lives and economy, Americans should feel secure when they use the Internet for business purposes, personal use, and commerce. Today, we will hear testimony from State and local officials about their efforts and needs, and how the Federal Government and private sector can assist them. Additionally, there are questions with regard to protecting privacy while enhancing law enforcement.

I would like to thank the witnesses for appearing before the Subcommittee today on such an important issue, and of course we all look forward to hearing your testimony in a few minutes. I will now recognize the Ranking Member, Mr. Scott of Virginia, for his opening statement.

Mr. SCOTT. Thank you, Mr. Chairman, and I also want to thank you for staggering the Subcommittee meetings so that Members can participate in all of their Subcommittee hearings without having to try and be in two places at the same time.

And I would also like to recognize on our side the gentleman from California, Mr. Schiff, who is officially attending his first meeting of this Subcommittee, although you have been kind enough to allow him to participate in previous meetings in the expectation that his formal membership would be confirmed. And I would like to welcome the gentleman from California.

Mr. SMITH. We all welcome Mr. Schiff, and it is nice to have him officially with us. As you said, Mr. Scott, we were never quite sure before but we did include him.

Mr. SCOTT. Thank you. I am pleased to join you in convening this hearing on State and local efforts to combat what is referred to as cyber crime or crimes committed through the use of electronic communications.

The field of electronic communications is rapidly evolving. During my relatively short tenure in Congress, we have moved from only speculating about the vast potential of the World Wide Web or the Internet superhighway to depending on it for the efficient conduct of daily congressional operations. We all rely heavily on the Internet for communicating with staff in our various offices and

for the efficient conduct of many routine activities, personal activities like paying bills and other such uses.

Given this rapidly growing dependency on electronic communications, the Congress and the rest of the Federal Government is just as subject to cyber crime as any other user, so we have just as much of a stake as anyone else in preventing cyber crime. Crimes such as theft or destruction of property, whether committed over the Internet or through other means, should be dealt with as such.

We have many laws on the books already, State and Federal, for dealing with such crimes. While I remain open to hearing proposals for additional crimes and penalties, I would hope that such additions are based on findings that they are necessary to effectively prevent crimes through electronic communications, rather than merely sending a message, which we have done in other areas of criminal law.

There is much the Federal Government can do and should do to assist State and local governments in addressing cyber crime. Providing funding for training and equipment, and lending technical assistance and cooperation to local and State law enforcement, are some ways. And, as you have indicated, the jurisdictional problems in cyber crime create new challenges for us.

While there may be holes in the Federal laws which prevent effective enforcement, and any such holes must be addressed, we must be vigilant to ensure that our zeal to address cyber crimes does not unduly constrain our privacy and individual freedoms, nor innovation. Unnecessary monitoring and oversight by law enforcement authorities could only stymie technology innovation. It could also infringe upon reasonable expectation of individuals to privacy and individual freedoms.

Most people expect the same kinds of privacy protection in their electronic communications as they receive with their mail and phones. In the absence of probable cause to believe that serious criminal activity is occurring, there is generally no right to invade mail or phone use, and I see no reason why we shouldn't have the same approach with electronic communications in balancing our need to ferret out crime with our privacy and individual rights as we do with mail and phones.

So it is my hope, Mr. Chairman, that before we identify what crimes we can add, that we first identify the problem and all of the potential solutions. To any business or individual requesting that the Federal Government be given more law enforcement oversight over electronic communications, I say we have to be careful as to what we ask for.

I was made aware of a case where one business accused a rival business of sabotaging its computer operations. In investigating the matter, the police confiscated all of the computers of the accused business, thereby essentially putting it out of business. Even though the charges were later dropped, the accused business lost several months of business and spent thousands of dollars for legal and other expenses incurred in trying to get its computers back. Obviously, that kind of cure was worse than the disease.

So I look forward to the testimony by witnesses today on what is occurring with respect to the issue of cyber crime at the State

and local level, and what the Government, the Federal Government might do to assist. Thank you, Mr. Chairman.

Mr. SMITH. Thank you, Mr. Scott.

Are there any other Members who wish to make an opening statement?

If not, we will proceed, and I will introduce the witnesses in the order in which they will testify: Mr. Ronald R. Stevens, Senior Investigator, Bureau of Criminal Investigation, New York, New York; Mr. Michael T. McCaul, Deputy Attorney General for Criminal Justice, Austin, Texas; and Mr. Joseph I. Cassilly, State's Attorney, Harford County, Bel Air, Maryland.

We welcome you all, and Mr. Stevens, if you will begin.

STATEMENT OF RONALD R. STEVENS, SENIOR INVESTIGATOR, BUREAU OF CRIMINAL INVESTIGATION, NEW YORK, NY

Mr. STEVENS. Thank you. Chairman Smith, Congressman Scott, and Members of the Subcommittee, my name is Ron Stevens. I am here representing the State of New York as the Director of the Computer Crime Unit for the New York State Police. I thank you for this opportunity to testify with regard to the current state of cyber crime in New York and what needs to be done in the future to address this growing problem.

The highest priority of Governor George Pataki protection and well-being of the citizens of New York State. The New York State Police, along with more than 500 local police departments, are committed to fulfilling this mission. As one of the 10 largest law enforcement agencies in the Nation, the New York State Police employs approximately 5,000 people in more than 200 locations statewide, including 1,000 investigative specialists. The New York State Police is a full service agency which also operates one of the Nation's leading crime laboratory systems, providing criminal justice agencies with state-of-the-art forensic analytical and investigative capabilities along with expert testimony.

The New York State Police Computer Crimes Unit was formed in 1992 to provide investigative and forensic capability in cases involving the use of computers and technology. A large portion of the unit's case work includes traditional crimes such as narcotics trafficking, gambling, homicide, sexual assault, and stalking, which can all be facilitated by the use of technology.

Law enforcement efforts directed toward cyber crime in New York State are focused in five primary areas. First, the forensic analysis of digital evidence. This is an evolving discipline in which the New York State Police is working to develop standard procedures and protocols statewide.

Next is critical information systems protection. In this area of growing concern, the New York State Police and the Office for Technology have developed a plan to respond to the increased number of threats to Government-owned computer systems.

The third area is child exploitation. The New York State Police, the Attorney General's Office, and the Division of Criminal Justice Services were among the first grant recipients in the Internet Crimes Against Children's Task Force program, working cooperatively with local, State and national efforts.

Fraud and identity theft are fourth, and account for more than 1,000 complaints received by New York agencies.

Finally, and no less significant, is training. The New York State Police as well as others are striving to meet the diverse training needs of law enforcement required to combat the proliferation of technology-enabled crime.

These five areas represent unique challenges for law enforcement. The speed and anonymity of the Internet allows criminals to commit crimes across geographic and jurisdictional boundaries. Investigations in this environment require partnership, cooperation, and information sharing between government at all levels, the private sector, and academia.

Agencies fighting cyber crime need strategies to train, retrain personnel who are in high demand in the private sector. The resources available to address these problems are severely inadequate, generally exceed those of most local agencies, and could not realistically be deployed by Federal agencies within the State. The New York State Police has accepted a central role in developing a coordinated cyber crime approach to address these needs.

The New York State Police and the Office for Technology have taken the first step in reaching this goal by developing a multi-agency plan to protect State computer systems and to respond to identified emergencies. This plan links a technical emergency response team and an information sharing and analysis center, the statewide deployment of highly trained investigators, and a facility to provide forensic analysis, training, program development, and legal research. Centrally headquartered in Albany, New York, this plan provides the framework to incorporate current law enforcement efforts and capabilities from all regions of the State.

A coordinated statewide initiative to fight cyber crime will require funding strategies that emphasize cooperative effort. We support the Computer Crime Enforcement Act of 2000, the Paul Coverdell National Forensic Science Improvement Act of 2000, and continued funding of the Internet Crimes Against Children's program, the National Cybercrime Training Partnership, and legislation which would improve the legal process that law enforcement must utilize in responding to cyber crime.

Mr. Chairman, I would like to thank the Committee for allowing me to share with it the issues regarding cyber crime in New York State. I look forward to continuing to work with you and the Members of your Subcommittee. At this time, I would be pleased to address any inquiries that you may have.

[The prepared statement of Mr. Stevens follows:]

PREPARED STATEMENT OF RONALD R. STEVENS

INTRODUCTION

Chairman Smith, Congressman Scott and members of the Subcommittee, my name is Ron Stevens, and I am here representing the State of New York as the Director of the Computer Crime Unit for the New York State Police. I thank you for this opportunity to testify with regard to the current state of Cybercrime in New York State, and what needs to be done in the future to address this growing problem.

The highest priority of Governor George Pataki is the protection and well-being of the citizens of New York State. The New York State Police, along with more than 500 local police departments across the state, are committed to fulfilling this mission. As one of the ten largest law enforcement agencies in the nation, the New

York State Police employ approximately 5000 people in more than 200 locations statewide—including 1000 investigative specialists in the Bureau of Criminal Investigation. The New York State Police is a full service police agency, which also operates one of the nation's leading Crime Laboratory Systems providing criminal justice agencies across New York with state-of-the-art forensic analytical and investigative capabilities and expert testimony.

The New York State Police fully understands and agrees that to successfully combat Cybercrime, law enforcement cannot "do it alone." The ramifications of a "connected" society, and the rapid proliferation of computers and the Internet, require that law enforcement work in a collaborative and coordinated manner. That is why the New York State Police has been diligently building relationships with organizations at the State, Local, and Federal levels. We have close working relationships with local police departments and District Attorneys' offices. We participate in regional and statewide task forces, including the New York Electronic Crimes Task Force, and take part in cooperative efforts with the New York State Division of Criminal Justice Services, Office for Technology, and Office of the Attorney General. The New York State Police is involved in training and research efforts with the State University of New York and other colleges and universities, as well as the National Law Enforcement and Corrections Technology Center. We participate in a number of national initiatives including the Scientific Working Group on Digital Evidence (SWGDE), the National Cybercrime Training Partnership (NCTP), and the FBI InfraGard program. We work cooperatively with the National Institute of Standards and Technology (NIST), the National Center for Forensic Sciences (NCFS), the National Infrastructure Protection Center (NIPC), and the American Society of Crime Laboratory Directors (ASCLD).

As one of the first law enforcement agencies to respond to the threats posed by the techno-criminal, the New York State Police launched the Computer Crime Unit in 1992. The Unit was created to provide investigative and forensic capability in investigations involving the use of computers and technology to facilitate crime. The primary function of the Computer Crime Unit is to bridge the communication gaps that exist between investigating police officers, prosecutors, and computer experts by providing the technical expertise and assistance needed.

WHAT WE ARE DOING TODAY

Many of the crimes that law enforcement confronts everyday are beginning to appear in the digital world. Criminals have adapted to the information age very quickly. More and more traditional crimes such as those involving narcotics trafficking, gambling, auto theft, homicide and assault, stalking, child pornography, fraud, and identity theft are facilitated by the use of technology. As criminals continue to utilize these evolving technologies, it is imperative that all levels of law enforcement are able to adequately respond to this elusive threat.

The Computer Crime Unit currently has five primary areas of responsibility—including forensic analysis, computer network and information systems security breaches, Internet crimes against children, fraud and identity theft, and training and research—challenges faced equally by law enforcement agencies statewide.

Forensic Analysis

Forensic examination of digital evidence can be crucial in the investigation of crimes facilitated by the use of technology. A growing number of investigations involve crime where critical evidence is stored on digital media such as computer hard drives. Whether the case is criminal, civil or administrative, processing digital evidence requires technically skilled personnel with specialized training and equipment. As the volume and complexity of casework grows, it will become increasingly important for additional resources to be allocated in a more efficient and effective manner.

Since 1997, the Computer Crime Unit has received more than 600 "containers" of evidence for forensic analysis. A container of evidence could consist of hundreds of removable media, a laptop computer, or a network server containing multiple disk drives. At present, there are 150 containers onsite awaiting processing. Requests for analyses are received daily, with urgent and time-sensitive cases receiving top priority. Accordingly, evidence in important investigations is analyzed and completed in a short period of time. However, low priority cases tend to have slower processing times due to the sheer volume of cases and available resources. It would take approximately 18 months to clear just the pending cases at current staffing levels, if no additional cases were received.

The fledgling discipline of computer forensics is at a point where the lack of accepted standards and procedural uniformity has prompted independent responses from a myriad of law enforcement agencies at the State, Local, and Federal levels.

If this haphazard approach continues, defense challenges could call into question the credibility of computer forensic analysis due to the lack of standardization. The science of computer forensics must evolve to meet the same standards of evidence that have been established for other forensic disciplines such as fingerprinting, ballistics, drugs, and DNA.

We need to ensure that standardized operating procedures in the field of computer forensics are established and incorporated into the training of forensic examiners across the nation. Population, geography, type and level of crime, as well as existing resources need to be evaluated prior to developing future computer forensic laboratories. In addition to the New York State Police Computer Crime Unit, law enforcement in Western New York and the New York City Metropolitan area are developing centralized forensic capabilities. The activities of all laboratories should be closely coordinated to ensure the development of generally accepted standards. At the same time, individual laboratories must be linked to the investigative mission of their respective region.

Computer Network and Information Systems Security Breaches

The reliance on computer interconnectivity has increased the risks associated with the Internet and computer network use. Malicious and unlawful cyber attacks in both the private and public sectors are becoming increasingly prevalent and of greater concern to mainstream society.

One of law enforcement's newest challenges is responding to attacks on public and private sector computer networks and information systems. Those at greatest risk are the networks and systems linked to state and national critical infrastructures, including information, communication, finance, energy, and transportation.

As society begins to accept law enforcement's role in our connected world, it is increasingly likely that law enforcement will become the "first responder" to cyber-based attacks. This will require the use of specialized technical and investigative personnel with a sound understanding of computer technology and advanced forensic analysis. Coordinated public sector resources must work with private sector interests and must be available in multiple jurisdictions in order to effectively protect our vital infrastructures.

In the State of New York, we have embarked on a multi-agency initiative focused on addressing cyber-based vulnerabilities. The New York State Police and the Office for Technology have worked in concert to develop a plan to address the increased risk of network and systems intrusion. The plan calls for the development of end-to-end detection and response capability thus enabling the State to identify and analyze attacks on government-owned computer networks and initiate appropriate technical and law enforcement measures when required. The plan also calls for the State to make every possible effort to ensure that an individual's liberties and privacy rights are protected.

Internet Crimes Against Children

The threat to our children from predators who hide their identity behind the veil of technology is greater than ever. Law enforcement in every state must act swiftly and decisively to protect innocent and vulnerable potential victims.

As a result of a preexisting multi-agency initiative, New York State was one of the first to receive a federal grant from the Office of Juvenile Justice and Delinquency Prevention (OJJDP), which created the NYS Internet Crimes Against Children (ICAC) Task Force (FY1999—$284,760; FY2000—$256,250; FY2001—$256,250). This dedicated multi-agency initiative—comprised of the New York State Police, Attorney General's Office, and Division of Criminal Justice Services—investigates computer-enabled crimes that exploit children. In addition, the task force works to promote standardized investigative techniques, trains law enforcement personnel, and enhances public awareness. By cooperating with 30 similar task force operations nationwide and local agencies that have received ICAC satellite grants, the NYS ICAC Task Force has been able to successfully investigate, arrest, prosecute, and incarcerate predators who target children.

Ever increasing caseloads—currently more than 1,000 active ICAC investigations in New York State alone—require more cooperation and centralized coordination. Mechanisms for coordinating and sharing information about undercover operations within each state must be improved to ensure officer safety and the efficient use of law enforcement resources.

A recent federal evaluation of the ICAC program made several recommendations. One critical recommendation addresses capacity building for both forensic analysis and training in response to the growing number of reported cases. The forensic needs and investigative skills required in ICAC investigations are the same for other crimes involving the use of technology, and must be addressed in coordination

with efforts in other program areas. Another recommendation proposes that a major ICAC grant be directed to each state. Quickly identifying, arresting, and prosecuting these predators will protect potential future victims. As the volume of cases grows, we need to ensure that there is a centrally coordinated point of contact in each state to advance multi-jurisdictional investigations.

Fraud and Identity Theft Investigation

Fraud investigations involving a "petty crime" are often indicative of more serious and far-reaching illegal activity. The ease and speed of the Internet can be used to facilitate fraud, enabling criminals to commit crimes with relative impunity. Scams of this type can be quickly replicated and disseminated worldwide.

Victims of these techno-crimes are now able to report fraudulent activity on a secure web site administered by the Internet Fraud Complaint Center (IFCC)—a joint initiative between the FBI and the National White Collar Crime Center. Complaints are then forwarded to all law enforcement agencies that have jurisdiction. The early success of this IFCC program illustrates the willingness of the public to report fraudulent activity to the proper authorities. Already more than 1,000 complaints have been referred to the New York State Police, and it is projected that this number will grow exponentially as IFCC continues to promote its program and increase its capacity to receive complaints.

The New York State Police has already created a database to record and analyze these IFCC complaints. Additional resources are needed to develop a systematic and coordinated response plan to disseminate complaints to the appropriate law enforcement agencies.

Cyber criminals are now preying upon individuals as well as businesses. The Internet is a venue that can be used to obtain extensive personal and financial information that, if in the wrong hands, can be used to perpetrate crime.

Recently, there was a case in New York City where an unscrupulous individual used the personal information of more than 200 of the wealthiest people in America to fraudulently obtain credit or services in the victim's name. This high-profile case is just one example of the identity theft complaints that law enforcement receives on a daily basis. In the year 2000, the Federal Trade Commission reported more than 2500 victims of identity theft in New York State.

Training and Research

The demand for highly trained and skilled personnel to investigate computer-enabled crimes is tremendous. This problem is compounded by the rapid advances in technology, which make continual training a necessity. In addition, there is a shortage of qualified instructors available to deliver law enforcement training in this area.

The Computer Crime Unit has provided instruction to thousands of law enforcement personnel throughout the State. At the same time, other law enforcement agencies are engaged in similar training programs. Consequently, duplicative training programs are emerging without coordination. These training efforts must be streamlined in a cooperative manner with delivery channels that result in high-quality instruction and training.

The United States Department of Justice currently funds the National Cybercrime Training Partnership—a consortium of experts from government, academia, and the private sector. New coursework is being developed based on the knowledge, skills, and abilities required today in the field of computer crime. One goal of the partnership is to identify existing, government-owned training and make it available at the local level in each state. Through "train the trainer" and distance learning programs, and in cooperation with academia, these modules must be incorporated into law enforcement training and academic degree programs.

WHAT MAKES THIS AREA SO CHALLENGING?

The broad reach of the Internet, which connects millions of people worldwide, presents a number of unique challenges to law enforcement in the fight against Cybercrime. Technologically sophisticated criminals can exploit the Internet's speed and distributed nature to commit crime and wreak havoc without regard to geographic and jurisdictional boundaries. A single perpetrator is able to anonymously take advantage of millions of vulnerable computer neophytes with relative ease. Law enforcement's dilemma is further complicated by the rate at which technological innovations evolve.

The nature of Cybercrime necessitates that law enforcement overcome institutional resistance to information sharing. Improving existing relationships and forging new partnerships, inside and outside of law enforcement, will improve every po-

lice agency's ability to exchange information in an expeditious manner. In so doing, law enforcement will be in a better position to investigate crime.

Attracting qualified candidates in the field of Cybercrime and computer forensics is difficult given the higher salaries offered by the private sector for similar skills. This amplifies the challenge for law enforcement agencies that seek to blend the stability and deployment flexibility of sworn personnel, with the technical expertise of civilian analysts. In addition, this rapidly expanding and evolving field requires personnel to receive training on a continuous basis in order to keep pace with the cybercriminal.

It is neither efficient nor practical for New York State to expect over 500 local police departments to investigate computer crimes and conduct forensic analyses. Most of these small local police departments, many with staffing levels of less than 10, lack sufficient resources needed to provide a comprehensive response.

Accordingly, the New York State Police with its statewide reach, investigative knowledge and expertise in the field of computer crime, make it the logical choice to play a central role in the development and operation of a coordinated Cybercrime initiative in New York State.

WHAT DO WE NEED TO DO IN THE FUTURE?

Fighting Cybercrime requires a coordinated approach, which unites local resources with those at the state and national level. Government must work cooperatively to ensure that statewide initiatives to fight Cybercrime are not duplicative. New York State, and others, must fit into a coordinated national plan, which ensures that staffing, equipment, and training resources are maximized, and provides a mechanism to share vital information. The federal government should work cooperatively with states to develop statewide initiatives in an effort to advance a systematic approach.

As part of an effort to develop a comprehensive and coordinated statewide initiative, the New York State Police and the Office for Technology took the first step toward meeting this goal by developing a multi-agency plan to protect the State's interconnected information systems.

This framework provides the mechanism by which the Office for Technology can secure the State's information systems, conduct network analysis, share information, and provide technical emergency response. Once a criminal act is identified, the New York State Police would mobilize the requisite investigative and forensic resources.

Specifically, the New York State Police would deploy highly trained investigative resources regionally around the State to investigate information system threats and crimes involving technology. These regional investigative units would be supported by a centralized operation with a wide range of services. A computer forensics laboratory would process large quantities of digital evidence in an expeditious manner, while meeting the most complex analytical challenges.

Another unit would conduct Cybercrime training initiatives, program development, and legal research and analysis. This unit would be responsible for training members of the State Police, and would work with other agencies to develop statewide training standards. In addition, an onsite legal expert would examine and research the complex challenges which accompany Cybercrime investigations, and at the same time, work closely with prosecutors during criminal investigations, proposing legislation and regulation as necessary.

The proposal also calls for highly trained State Police liaison personnel to be located at the Office for Technology to coordinate and initiate the necessary law enforcement response to a network intrusion or cyber attack.

Overall, this collaborative, multi-agency information systems protection proposal provides the foundation to build a statewide, coordinated Cybercrime initiative in New York State.

Building a framework of this type requires that the unique strengths and capabilities of various regions be considered. These include:

Western New York:

- academic and research institutions in Buffalo and Rochester,
- a number of experienced Cybercrime investigators and prosecutors,
- geographic proximity to our Canadian partners in Ontario, and
- a newly developed Regional Computer Forensic Laboratory, established by the United States Attorney's Office in the Western District of New York.

Upstate New York:

- the center of New York State government,

- major academic and research institutions, including the University at Albany and Rensselaer Polytechnic Institute,
- the hub of the NYeNet, a statewide fiber optic network which supports the New York State E-Government Initiative,
- the New York State Police Forensic Investigation Center, along with the headquarters of our major investigative operations into the areas of narcotics, auto theft, and organized crime which operate in close cooperation with governments in New England, New York City, and Quebec, Canada, and
- major research centers at Syracuse University, Cornell University, and the Air Force Research Laboratory in Rome, New York which are vital resources in the development of information assurance and computer security technologies,

New York Metropolitan Area:

- the hub of international commerce,
- home of the United Nations,
- major research universities,
- the multi-agency New York Electronic Crimes Task Force, and
- the New York City Police Department, the nation's largest law enforcement agency

WHAT CAN THE FEDERAL GOVERNMENT DO TO HELP?

The national and international ramifications of Cybercrime suggest that the federal government develop funding guidelines promoting the adoption of a coordinated, statewide approach to address the growing threat of Cybercrime.

Computer Crimes Enforcement Act of 2000

We support the Computer Crimes Enforcement Act of 2000 (P.L.106–572), which was signed into law on December 28, 2000, and urge Congress to fund this legislation and consider additional funding targeted to those states that develop a statewide coordinated Cybercrime initiative.

Paul Coverdell National Forensic Sciences Improvement Act of 2000

We support the Paul Coverdell National Forensic Sciences Improvement Act of 2000 (P.L.106–561), which was signed into law on December 21, 2000, and urge Congress to appropriate funds specifically for computer forensic laboratories, with funding again aimed at states that develop coordinated Cybercrime initiatives.

Office of Juvenile Justice and Delinquency Prevention (OJJDP)

Funding for Internet Crimes Against Children

We support continued funding for the Internet Crimes Against Children program, through the Office of Juvenile Justice and Delinquency Prevention (OJJDP), and urge Congress to direct major grant awards to each state. In addition, funding for forensic capacity should be coordinated with other funding efforts in forensics, and funding for training should be coordinated with the efforts of the National Cybercrime Training Partnership and other training efforts.

National Cybercrime Training Partnership (NCTP)

We support continued funding for the National Cybercrime Training Partnership program to develop curricula and educate instructors. We urge Congress to establish a dedicated Scholarship Fund that would enable critical personnel from state and local government to participate in existing coursework identified by the partnership.

CLOSING REMARKS

Mr. Chairman, I would like to thank the committee for allowing me to share with it the facts regarding Cybercrime in New York State. I look forward to continuing to work with you and the Members of your Subcommittee. At this time I would be pleased to address any inquiries you might have.

Mr. SMITH. Thank you, Mr. Stevens.
Mr. McCaul?

STATEMENT OF MICHAEL T. McCAUL, DEPUTY ATTORNEY GENERAL FOR CRIMINAL JUSTICE, AUSTIN, TX

Mr. MCCAUL. Thank you, Mr. Chairman. Let me first say it is good to see a fellow Texan in your position. And Members of the Subcommittee, I thank you for this opportunity to testify on the topic of cyber crime and efforts at the State level to combat it.

In my view, two factors have converged in recent years to bring about a major criminal justice problem, and that is the widespread use of computers and the Internet to commit crimes and a critical lack of resources. Last September, Attorney General John Cornyn launched the Texas Internet Bureau to address the rapid growth of cyber crime in Texas. Since that time, the investigators and prosecutors in our office have been faced with a daunting array of cases, from Internet-savvy child predators, online child pornographers, to computer hackers, identity thieves, and fraud online.

Modern day criminals have learned to exploit the Internet and leverage computer technology to reach a virtually unlimited number of victims while maintaining a maximum level of anonymity, and I have no doubt that the number and variety of computer crimes will continue to mount. It is projected that global e-commerce dollars will rise from $50 billion in 1998 to $1.3 trillion in 2003. The phrase "follow the money" applies not only to investors but to criminals as well.

Unfortunately, one of the biggest problems is that computer criminals are targeting the most vulnerable of our society, and that is the children. While the Internet has revolutionized the ways in which the world communicates, there is an equally awesome dark side to it. According to the Federal Bureau of Investigation, child pornography was virtually extinct prior to the advent of the Internet. However, with increased Internet usage in America and the world, there has been an alarming increase in child pornography cases.

According to the U.S. Postal Service. 40 percent of the offenders who have been arrested with child pornography downloaded from the Internet have already sexually assaulted minors. That is a staggering statistic.

The National Center for Missing and Exploited Children issued a report entitled "Online Victimization: A Report on the Nation's Youth." This report presents troubling and startling results. Based on interviews of 1,500 youths between the ages of 10 and 17, the report found that approximately one in five children received a sexual solicitation or approach over the Internet in the last year. One in four children had an unwanted exposure on the Internet to sexually explicit images, and 1 in 17 children were either sexually threatened or harassed.

A large portion of our case load in Texas involves the investigation of these online child predators. In one case recently investigated, a 25-year-old school teacher was arrested after he solicited sex from a person he believed to be a minor in a chat room entitled "Younger Girls for Older Men." A subsequent investigation revealed that the suspect had previously used the Internet to seduce a 15-year-old girl, and the suspect was rearrested and charged with three counts of sexual assault of a child.

Another case that our office handled involved a school shooting case in Brownfield, Texas, to show you how widely diverse these cases are. Our office became involved after the local police called for our assistance. They had a report that a student was hacking into the high school's computer system.

After we executed the search warrant, we found in the student's home a written narrative detailing a plan to shoot up the school and murder several students, a master key to the high school, and schematic plans of the high school. And the student was, in fact, hacking into the school's computer system. The investigation led to the prosecution of the juvenile, who is now serving time in a juvenile facility in Texas.

These cases demonstrate that computer crimes have serious consequences: the rape of a child, and a potential school massacre. If we are to stem the flood of cyber crime, State and local authorities must increase their enforcement efforts. Attorney General Cornyn's Texas Internet Bureau is a step in the right direction and, I believe, a model for the Nation, but it is only a first step.

I believe that any efforts aimed at helping State and local law enforcement authorities to combat cyber crime should be focused on three primary areas of concern: one, jurisdictional issues; two, cooperative initiatives; and, three, resources.

Traditional State and local law enforcement agencies have been keenly aware of the jurisdictional boundaries in which they operate. This model is very effective in handling local crimes where the suspect, the victim, and the crime scene are all in one jurisdiction. The Internet, however, is an environment without boundaries, an environment which enables criminals to victimize local populations from anywhere in the world.

Consider an example: a fraudulent scheme targeting Texas residents is perpetrated from a web site located in Ohio. Investigators don't know where the perpetrator lives, and in order to locate the suspect, we must issue a subpoena and serve that on the ISP in Ohio. Currently, there is no formal mechanism for service of process or compliance with the subpoena, so the ISP could completely ignore the subpoena altogether. Or Texas prosecutors might succeed in convincing the ISP to comply by obtaining help from local authorities in Ohio. The problem with this is that it would be a matter of professional courtesy and not one of a legal process.

This example illustrates the kind of jurisdictional hurdles often faced by State and local authorities, and the need for laws that provide for authority for out-of-State service of process and enforceability of that process.

I am convinced that the problem of computer crime cannot be addressed by any one level of government acting on its own. And while the Feds have taken the lead in this area, they cannot solve this problem alone, and the States need to step up to the plate. It is simply not enough to react to the problem. Law enforcement must learn to interact if we are to triumph over network crime.

The vast scope of the Internet and its increasing pervasiveness demands that governments develop partnerships and joint initiatives. Recently the National Association of Attorneys General, or NAAG, and the Department of Justice's Computer Crime and Intellectual Property Section, worked together to create a Computer

Crime Point of Contact list that contains the name of the investigator and prosecutor for each State. These individuals have agreed to serve as contact points when investigators from out-of-State have questions during the course of a cyber crime investigation or prosecution.

In Texas our office has been involved in another joint initiative which I believe is most significant, and that is the creation of the North Texas Regional Computer Forensics Lab. This lab is a multi-agency facility that serves the computer forensics needs of all law enforcement agencies in a 137-county region surrounding the Dallas area.

Prior to the creation of the lab, there was about an 8 to 12 month backlog of seized computers that needed to be examined. Since the creation of the lab, that delay has been reduced to less than 1 month.

Mr. SMITH. Mr. McCaul, I have to interrupt you. I am tracking your statement, and unfortunately we are running short of time. Could I ask you to summarize the remaining part of your statement?

And let me also say to all the witnesses today that, without objection, your entire testimony will be a part of the record.

Mr. MCCAUL. Yes, Mr. Chairman.

I would like to say we have partnered with the FBI and the Commerce Department's Critical Infrastructure Office to host a conference this fall on cyber terrorism. I believe with the dawn of the Melissa virus and others, the threat to our national security by a rogue nation or a small group of anarchists by computers is really no longer futuristic, but rather is a present-day reality, and it is imperative that the Federal Government partner with the States to protect our critical infrastructure.

My last point, and I think perhaps most importantly in response to Congressman Scott's question about enacting new laws, I believe the area where we need the most help and where we don't need a new law enacted is in the area of the Computer Crime Enforcement Act. That was enacted into law.

That act provided for funding for the States, a grant program to assist State and local law enforcement. It also provided for $25 million over the next 4 years for the purpose of what we are discussing here today, and that is to help the State and local law enforcement authorities. I simply ask that the Congress appropriate the funding that the act authorized. Unfortunately, funding was never appropriated under this act, and I believe without that funding it is virtually impossible for us to do an effective job to combat cyber crime.

Thank you very much.

[The prepared statement of Mr. McCaul follows:]

PREPARED STATEMENT OF MICHAEL T. MCCAUL

Mr. Chairman and Members of the Subcommittee, I thank you for this opportunity to testify on the topic of cyber crime and efforts at the state level to combat it. Two factors have converged in recent years to bring about a major criminal justice problem: the wide spread use of computers and the Internet to commit crimes, and a critical lack of resources, especially at the state and local level, to combat computer-related crime. Last September, Attorney General John Cornyn launched the Texas Internet Bureau to address the rapid growth of cyber crime in Texas. Since that time the investigators and prosecutors at the Internet Bureau have been

faced with a daunting array of cases—from Internet savvy child predators and online child pornographers to computer hackers, identity thieves and computer fraudsters. Modern day criminals have learned to exploit the Internet and leverage computer technology to reach a virtually unlimited number of victims while maintaining a maximum level of anonymity, and I have no doubt that the number and variety of computer crimes will continue to mount.

Unfortunately, one of the biggest problems is that computer criminals are targeting the most vulnerable of our society—children. While the Internet has revolutionized the ways in which the world communicates, there is an equally awesome dark side. According to the Federal Bureau of Investigation, child pornography was virtually extinct prior to the advent of the Internet. However, with increased Internet usage in America and the world there has been an alarming increase in child pornography cases. According to the U.S. Postal Service, 40 percent of the offenders who have been arrested with child pornography downloaded from the Internet have sexually assaulted minors. The National Center for Missing and Exploited Children and the Crimes Against Children Research Center's June 2000 report entitled Online Victimization: A Report on the Nation's Youth presents startling and disturbing results. Based on interviews with a nationally representative sample of 1,501 youths ages 10 to 17 who use the Internet regularly, the report found:

- Approximately one in five children received a sexual solicitation or approach over the Internet in the *last year*.
- One in thirty-three received an *aggressive* sexual solicitation—a solicitor who asked to meet them somewhere; called them on the telephone; sent them paper mail, money, or gifts.
- One in four children had an unwanted exposure on the Internet to pictures of naked people or people having sex *in the last year*.
- One in seventeen children was threatened or harassed.
- Approximately one quarter of the children who reported these incidents were distressed by them.
- The interviewed children reported less than 10% of the sexual solicitations and only 3% of the unwanted exposure episodes to law enforcement, the Internet Service Provider, or a hotline.
- Only about 25% of the youth sexually solicited or approached told a parent and only 40% of those who experienced unwanted exposure to sexual material told a parent.
- Only 17% of youth and approximately 10% of parents could name a specific authority (such as the FBI CyberTipline, or an Internet service provider) to which they could make a report, although more said they had "heard of" such places.
- In households with Internet access, one third of parents said they had filtering or blocking software on their computer at the time they were interviewed.[1]

A large portion of the Texas Internet Bureau's case load involves the investigation of online child predators. In one case recently investigated by the Internet Bureau, a twenty-five year old school teacher was arrested by Austin police officers and Internet Bureau investigators after he solicited sex from a person he believed to be a minor in a chat room entitled "Younger Girls for Older Men." A subsequent investigation revealed that the suspect had previously used the Internet to seduce a fifteen year old girl, and the suspect was re-arrested on three counts of sexual assault of a child.

Internet Bureau investigators have been involved in other cases as well. For example, last March, an investigator from the Internet Bureau assisted local police in investigating a potential school shooting case in Brownfield, Texas. The Internet Bureau became involved after Brownfield police received a report that a student was hacking into the local high school's computers. When the Internet Bureau and local police searched the student's home, they discovered a written a narrative detailing a plan to shoot up the school and murder several students, a master key to the high school, and schematic plans of the high school. Investigators also learned that the student was, in fact, hacking into one of the school's computers. The investigation led to the prosecution of the juvenile who is now serving time in a juvenile facility in Texas.

---

[1] DAVID FINKLEHOR, KIMBERLY J. MITCHELL, & JANIS WOLAK, ONLINE VICTIMIZATION: A REPORT ON THE NATION'S YOUTH (The National Center For Missing and Exploited Children 2000) (June 2000).

These cases demonstrate that computer crimes have serious consequences—the rape of a child, and a potential school massacre. If we are to stem the flood of cyber crime, state and local authorities must increase their enforcement efforts. Attorney General Cornyn's Texas Internet Bureau is a step in the right direction, but it is only a first step.

I believe that any efforts aimed at helping state and local law enforcement authorities combat cyber crime should be focused on three primary areas of concern: (1) jurisdictional issues, (2) cooperative initiatives, and (3) resources.

JURISDICTIONAL ISSUES

Traditionally, state and local law enforcement agencies have been keenly aware of the jurisdictional boundaries in which they operate. City police officers patrol the city, county sheriff's deputies patrol the county outside of the city, and state police officers patrol the Interstate highway system. This enforcement model is very effective in handling local crimes—crimes where the suspect, the victim, and the crime scene are located within one jurisdiction. The Internet, however, is an environment without boundaries; an environment which enables criminals to victimize local populations from anywhere in the world. Consider an example: a fraudulent scheme targeting Texas residents is perpetrated from a website. The website is hosted on a computer in Ohio, and investigators are not sure where the perpetrator is located. In order to locate the fraudster, Texas prosecutors would likely issue subpoenas to the service provider in Ohio, but currently, there is no formal mechanism for service and compliance with this subpoena and the Ohio provider could choose to ignore the subpoena altogether. Texas prosecutors might succeed in convincing the service provider to comply by obtaining help from authorities in Ohio, but this would be a matter of professional courtesy and not legal process. In addition, because service providers often only temporarily maintain records of Internet activity, the delay caused by having to contact out of state authorities and obtain assistance may result in the deletion of the records sought.

This example illustrates the kind of jurisdictional hurdles often faced by state and local authorities investigating crime on the Internet. State and local authorities need laws that provide authority for out of state service of process and enforceability of that process.

COOPERATION AND COORDINATION

I am convinced that the problem of computer crime cannot be addressed by any one level of government acting on its own. It is simply not enough to react to this problem—law enforcement must learn to interact if we are to triumph over network crime. The vast scope of the Internet and its increasing pervasiveness demands that governments develop partnerships and joint initiatives. Recently, the National Association of Attorneys General ("NAAG") and the Department of Justice's Computer Crime and Intellectual Property Section ("CCIPS") worked together to create a "Computer Crime Point of Contact List" that contains the name of an investigator and prosecutor from each state. These individuals have agreed to provide their telephone numbers and to serve as the contact point when investigators from out of state have questions during the course of a cyber crime investigation or prosecution. A copy of this list is available on NAAG's website at *www.naag.org*.

In Texas, our office has been involved in another joint initiative—the creation of the North Texas Regional Computer Forensics Lab. The North Texas Regional Computer Forensics Lab is a multi-agency facility that serves the computer forensics needs of all law enforcement agencies in a 137 county region surrounding the Dallas metroplex area. The cases investigated and prosecuted by the Texas Internet Bureau often turn on evidence contained within computers, evidence that must be examined and analyzed by experts such as those at the North Texas Regional Computer Forensics Lab. Prior to the creation of the lab, however, there was an eight to twelve month back log of seized computers that needed to be examined. This meant that if an investigator developed probable cause to search a child pornographer's computer for evidence of child pornography, the investigation would be put on hold for almost a year while the computers were analyzed and evidence extracted. Since the creation of the North Texas Regional Computer Forensics Lab, that delay has been reduced to less than a month. Attorney General Cornyn is very proud that the Texas Internet Bureau has joined with the FBI and nine local police departments in creating this Lab as the resource it provides will greatly enhance Texas efforts to bring cyber criminals to justice.

Because we believe joint law enforcement efforts can have a truly awesome impact, our office is aggressively pursuing collaborations with all levels of law enforcement. For instance, the Texas Internet Bureau is working closely with the Dallas

Police Department and the Dallas County Sheriff's office in the Internet Crimes Against Children Task Force. Frequently, investigators from our office conduct joint investigations with the Austin Police Department's High Tech Squad or with the Texas Department of Public Safety's Special Crimes Division.

We are also working with federal agencies. In fact, we were able to attract a top cyber crime prosecutor, Reid Wittliff, from the Dallas US Attorney's office to head the Internet Bureau. Another one of our prosecutors has been selected for a fellowship sponsored by NAAG with funds received from the Bureau of Justice Assistance at the Computer Crime and Intellectual Property Section here in Washington. In prior years, representatives from three attorneys Generals' offices have gained valuable experience during the fellowship. If this years fellowship is funded, we see two benefits coming from it: first, our attorney will gain expertise and training in the area of computer crime and bring that experience to the Texas Internet Bureau, and second, our office will build a closer relationship with the Department of Justice. Following the success of the CCIPS fellowship, the Texas Internet Bureau has plans to start a similar internship program this Fall. We plan on creating two internship positions for local police officers who will come work at the Internet Bureau and gain experience and hands on training, and then take that experience back to their local departments after the internship.

RESOURCES

Joint partnerships of federal, state, and local law enforcement agencies such as the North Texas Regional Computer Forensics Lab are the solution to the problem of cyber crime—but these initiatives will not get off the ground without resources. Cyber crime fighting is an expensive endeavor. Technical equipment is expensive, and technology is rapidly changing. The cyber crook is likely to have up to date technology and law enforcement needs to keep pace with him. Funding for personnel is critical. Training an officer is costly. According to the Director of the North Texas Regional Computer Forensics Lab, it costs almost $35,000 to train one of their computer forensics examiners. And once officers are trained, retention becomes a problem as technically trained law enforcement officers are few and far between and often have offers to work at high-paying private sector jobs. The computer crime point of contact list mentioned earlier can be a tremendous resource, but only if the state contacts on the list have the resources and support needed to handle computer crime referrals. Simply put, the states need funding for personnel, training, and not just a one-time allotment, but on a recurring basis. Although Congress authorized money for computer crime investigations and forensics programs last year, the provisions went unfunded. The states desperately need this appropriation. Without it, cash strapped agencies will not be able to effectively investigate the computer crimes reported to them.

In sum, we believe an effective cyber crime strategy should include: new legislation aimed at breaking down jurisdictional barriers to cyber crime investigations; programs designed to foster multi-agency approaches to computer crime investigations and prosecutions; and finally, an increase in resources to law enforcement for use in cyber crime investigations and prosecutions. We are very pleased to see that Congress is concerned about this pressing criminal justice problem and we look forward to working with the Subcommittee in finding solutions to the growing computer crime problem.

Mr. SMITH. Thank you, Mr. McCaul.

Mr. Cassilly?

STATEMENT OF JOSEPH I. CASSILLY, STATE'S ATTORNEY, HARFORD COUNTY, BEL AIR, MD

Mr. CASSILLY. Thank you, Mr. Chairman, Members of the Committee. Thank you on behalf of the National District Attorneys Association, representing America's local prosecutors, for the opportunity to express our concerns on cyber crime. I am the Chair of the Cyber Crime Committee of the NDAA, and its representative on an FBI cyber crime working group to develop unified strategies to deal with this epidemic.

I have been a prosecutor for 24 years, elected to office five times. My office has handled numerous types of cyber crimes. I would like to highlight three areas of concern.

One, training and resources. As has been expressed by other witnesses, there is definitely a need for training. I would like to focus on what local prosecutors need. Computers have created new crimes, such as viruses and denial of service attacks, and provided innovative ways to commit old crimes.

With these problems have come development of new investigative methods, new laws regarding obtaining evidence, working in foreign jurisdictions, and learning a new vocabulary. For the prosecutor comes the task of presenting cyber evidence to judges and juries, and assessing losses for sentencing.

Since cyber crime is a relatively new area, there is a dearth of prosecutors with any knowledge in this area. We need funding to bring classes and speakers to the States and provide multidisciplinary training so that prosecutors, investigators, and technicians can learn together. A traveling curriculum could quickly give local law enforcement the tools we need to plan and react.

Along with this, we do not have the equipment needed to investigate and prosecute cyber offenses and present the cases in the courtroom. We need seed money to get the computer equipment and the skills to use it at the local level. We need intensive efforts to train prosecutors on handling cyber crimes.

Two, forensic labs. Mr. McCaul indicated the problems with forensic labs. One solution that I visited is the regional computer forensic laboratory in San Diego. The lab's physical set-up was acquired principally with Federal money, but it is staffed with law enforcement officers from 27 local, State, and Federal police agencies. This provides the top of the line resources to local law enforcement and leads to standardized procedures, interagency cooperation, and information sharing.

Contrast this with other places where competing Federal agencies have labs within miles of one another which do not share resources or experience, or cooperate with one another or with neighboring State and local labs. Please visit this lab and understand the work they do. Then Congress should take the lead to ensure that a series of these labs is developed to serve all levels of government.

The third area is standardization, first as it relates to laws. Congress needs to take the lead in uniform laws for securing evidence from out-of-State witnesses, ISPs, and record storage facilities. Federal laws should make it possible for and require Federal law enforcement and U.S. Attorneys to use their offices to assist local law enforcement in the preparation of subpoenas and warrants and the service of same, and to assist in the investigation of cyber crime, to obtain the evidence and relay it to the State. They could do this by possibly cross-designating local attorneys to act as Assistant U.S. Attorneys and give them access to the Federal courts, or by requiring Internet service providers to accept subpoenas from out-of-State as if they were issued from within their own States, without the necessity, as Mr. McCaul indicates, of going through the local prosecutor's office.

Second is laboratory standards. Why is this an issue for local prosecutors? Look at the thousands of hours of prosecutor preparation and court time for hearings in court after court to establish the scientific acceptability and reliability of DNA and DNA laboratory

procedures, to understand why a local prosecutor would be interested in a standard set of forensic procedures. Besides law enforcement, there are many other computer forensic laboratories.

Laboratory standards might best come from the National Bureau of Standards, with input from law enforcement, the IT industry, and others. A uniform set of standards would improve laboratory quality, and allow the prosecutor and the judge or jury to know that evidence they rely on was obtained with the best practices.

If our law enforcement efforts continue to develop in a random manner, our confusion will only be aiding criminals. On behalf of America's prosecutors, the National District Attorneys Association looks forward to working with you to fashion a solution. Thank you.

[The prepared statement of Mr. Cassilly follows:]

PREPARED STATEMENT OF JOSEPH I. CASSILLY

My name is Joe Cassilly and I am the elected prosecutor in Harford County, Maryland. I want to thank you on behalf of the National District Attorneys Association, representing the local prosecutors of this Nation, for the opportunity to give you our concerns on cyber crime. On behalf of our members I want to commend this Committee in pursing an area of vital importance to the citizens and our system of criminal justice.

I am also the Chair of the Cyber Crime Committee of the National District Attorneys Association and have served in various capacities within that organization since 1996. I also serve as the NDAA representative on FBI cyber crime working groups as we attempt to develop unified strategies to fight this epidemic. In addition to these national offices, I am also the president of the Maryland State's Attorneys Association.

The views that I express today represent the views of that Association and the beliefs of local prosecutors across this Country. Let me assure you that local prosecutors need your help in tackling this every increasing criminal threat.

To place my remarks in context—on both a local level and on the national stage let me briefly tell you about my jurisdiction. Harford County is northeast of Baltimore and lies along the Susquehanna River. It has a population of about 225,000 people living in towns, suburban and rural areas with one large military base within our jurisdiction. I have been prosecutor for 24 years and honored to serve in my current office for 19 years, having been elected to office 5 times. I still actively try cases as well as supervise a staff that includes 23 deputy and assistant state's attorneys. Annually, my office handles more than 2500 felony cases.

During my tenure as a prosecutor, my office has investigated various computer crimes including cyber stalking, bomb and shooting threats in schools, child pornography, identity theft and on-line fraud schemes. In the course of those investigations I have worked with local, state and federal law enforcement agencies as well as security personnel from the information technology industry.

When we think of "cyber crimes" we frequently look at the headlines of international bugs and viruses—let me personalize this for you.

Recently, one of my police departments was contacted by a teenager in Arizona and told that a teenage boy on an Internet Relay Chat room had threatened a shooting at a Harford County high school. Working through the night the police with assistance from AOL were able to begin to trace back the message. Unfortunately, the police had to wait until another ISP opened the next morning to complete the information and arrest the juvenile. Due to the opening time of school, we were unable to obtain the information before students began arriving and armed, uniformed police officers had to be stationed around the school as a precaution. Needless to say parents and students were quite upset.

In another case, the teenage daughter of a local elected official met a man in a cyberspace chat room. She agreed to meet him. He came in from New York. He drugged her drink, undressed her and videotaped her. When he set up a later meeting, the police were waiting. A search warrant executed in his residence found other victims.

And finally—child pornography. Nothing is as truly revolting and heartbreaking as to get into hidden files on a computer disk only to find movies and still photos of a small child being brutalized, degraded and scarred for life. The demand for

these images is an international scandal, which starts each time with one child who needs the protection of local police and prosecutors.

I would like to highlight three areas of concern from the perspective of local prosecutor and use those as the catalyst for any further areas of discussion that you wish to pursue. They are the need for resources and training at the local level; the need for regional forensic laboratories and, lastly, the need for standardization of laws and forensic efforts across the nation and even internationally.

TRAINING AND RESOURCES

Crime once required a physical presence but it doesn't anymore. Computers have created new crimes, such as viruses, denial of services attacks, and hacking. Computers provide innovative new ways to commit old crimes; such as theft, pornography and drug dealing. With these problems have come the development of new investigative challenges, contacting hundreds, even thousands, of victims from a single internet solicitation, defining jurisdiction of a crime that spans dozens of states or countries, getting cooperation from service providers, record storage sites and investigators in other states or countries, new laws regarding obtaining evidence or working with laws in foreign jurisdictions. Learning a new vocabulary of IP, IT, URL, encryption, steganography and volatile memories. Additionally for the prosecutor comes the tasks of having courts recognize computer forensic laboratory techniques and technicians, presenting evidence to judges and juries and assessing the losses for sentencing.

The majority of law enforcement focus will be on financial records, location of stolen property, child pornography, terrorist threats, stalking, trespasses and other thefts and frauds. One or two people on LAN's using the WAN to defraud other smaller users at the other end generally perform these.

One of the major problems of state law enforcement has nothing to do with technology but is basic jurisdiction and cost efficiency. The majority of frauds and thefts are under $100,000 and usually involve parties resident in different states. The federal authorities have little interest in cases under $1 million—so most of the caseload will naturally fall to the states. But will a Prosecutor be willing or have the resources to extradite on a $5,000 theft case?

We also have a lot to learn about search and seizure law as applied to the cyber world. In seizing a computer system it is important to have a very expansive list of items that can and should be seized. Off machine disk drivers can contain more data than the hard drive but if you don't specify them in the warrant you miss crucial evidence.

We also have to recognize that chain of evidence rules still apply and may even be more difficult as hard-and-soft ware goes through various forensic laboratories. A challenge here is when we have to use non-law enforcement organizations (such as the technology industry themselves); then we have to ensure they fully understand the requirements before any thing is actually turned over to them for analysis.

The sheer numbers of cases, which are increasing exponentially every year, is beyond the capability of any one law enforcement agency; yet at the state and local level, where the bulk of our law enforcement capabilities are concentrated, we are particularity unprepared to deal with the sophisticated concepts of cyber crime.

Usually, new prosecutors are trained by more experienced prosecutors in an office, but since cyber crime has only appeared in the last decade there is a dearth of prosecutors with any knowledge in this area. There is some training available at for example the National White Collar Crime Center in West Virginia, but what we need is funding to bring classes and speakers into the states and provide multi-disciplinary training so that prosecutors, investigators and technicians can learn together.

I would note that NDAA's "think tank," the American Prosecutors Research Institute has done some excellent training on a number of complex topics but has not been provided opportunities to work with prosecutors in this emerging and difficult area. A traveling curriculum could quickly give local law enforcement the tools we need to plan and react. It's impossible to convince a jury of something that you don't understand yourself!

Many of our prosecutors have better computers on their kid's desks at home then they do in their offices—some do not even have computers in their offices. In addition you need computers, projectors, zip drives and specialized software to present these cases in the courtroom. By and large we do not have the equipment needed to investigate and prosecute cyber offenses and even when we do it is often out dated compared to the latest equipment that many cyber criminals use.

Bottom line—we need help in seed money to get the computer equipment and the skills to use it at the local level. We need intensive efforts to train prosecutors on trying cases in which computers are used to facilitate the offense.

Congress receives many pleas for help but the nature of cyber crime demands national attention.

FORENSIC LABS

Part of the investigative work necessary to identify and prosecute a cyber criminal is the forensic work that must be done to capture and preserve evidence of the criminal activity. Just as a forensic investigator identifies and analyzes evidence at a "traditional" crime scene, evidence from computers must be identified and analyzed. This is, obviously not an easy task and the wait for the work to be done now can be unreasonable. And while we wait for forensic work to be completed cyber criminals may be free to victimize others.

I would like to call the Subcommittees' attention to one solution—that of the regional computer forensic laboratory that has been established in San Diego. The lab's physical set-up was acquired principally with Federal money but it is staffed with law enforcement officers from 27 local, State and Federal police agencies. Not only does this provide the top of the line resources to local law enforcement, but also it leads to standardized procedures, and inter-agency cooperation and information sharing. The lab also contains a classroom that provides the training we need. I would urge that you visit this lab and understand the complexity of the work they do; then I would urge that Congress take the lead to ensure that a series of these labs is developed to serve all levels of government.

This should be contrasted with other places where competing Federal agencies have labs within miles of one another, which do not share resources or experience or cooperate with one another or with neighboring State and local labs.

Years ago, when DNA first became useful as evidence in criminal cases we were slow to realize it's potential to both condemn and clear individuals of criminal activity. And because we were slow we did not develop the laboratory capacity at either the national or state levels to accomplish the necessary forensic capability to support our criminal justice system. We need to learn from this and make sure that we develop forensic facilities for cyber crime before it over whelms our system.

STANDARDIZATION

Standardization relates to two areas.

First, laws. Just as the action of Congress is responsible for a uniform .08 alcohol reading across the United States, Congress could take a lead in uniform laws for securing evidence from out of state witnesses, ISP's and other record storage facilities. For example, America On Line's corporate headquarters are across the Potomac in Loudon County, Virginia. Loudon County is around 200,000 citizens.

According to the Commonwealths Attorney for Loudon County, a day does not go by that his office is not called upon for information and assistance to serve subpoenas, warrants and court orders on AOL for prosecutors from New York to California. In other words the taxpayers of Loudon County are supporting the efforts in other states to fight a national crime problem. This inequity is repeated in many other local prosecutors offices where Internet service providers are located.

Federal laws should make it possible for Federal law enforcement and U.S. attorneys to use their offices to assist in the preparation of subpoenas and warrants and the service of same to assist local law enforcement in the investigation of cyber crime to obtain the evidence and relay it to those states.

Second, laboratory standards. Why is this an issue for local prosecutors? One only has to look at the thousands dollars and thousands of hours of prosecutor preparation and court time for hearings to establish the scientific acceptability and reliability of DNA and the accompanying laboratory procedures for its analysis in court after court to understand why a local prosecutor would be in a standard set of forensic procedures. Since besides law enforcement there many private, national security and other computer investigators and forensic laboratories, laboratory standards might best come from the National Bureau of Standards with input from law enforcement, the IT industry and others.

A uniform set of standards would improve laboratory quality and from a prosecutor's perspective allow the prosecutor and the judge or jury to know that evidence they rely on for guilt or innocence determinations was obtained with the best practices and is not likely to be attacked in court

It is crucial that we have the ability to investigate and prosecute cases involving cyber technology—our citizens deserve nothing less. We cannot do this unless we adopt courses of action that afford a unified approach to the problem. If out law en-

forcement efforts continue to develop in a random manner, as they are at this time, we will not be protecting out citizens and our confusion will only be aiding criminals.

On behalf of America's prosecutors I, and the National District Attorneys Association look forward to working with you on limiting and even ending crimes committed using advanced technology.

For further information contact
Jim Polley
Director, Government Affairs
National District Attorneys Assn
(703) 519–1651 or james.polley@ndaa-apri.org

Mr. SMITH. Thank you, Mr. Cassilly.

The thrust of my questions is going to be to ask each one of you what you think the specific problem is that you confront, and also what you think the solution is, in the way of either changing current laws or perhaps drafting new laws. Mr. Stevens, in your testimony you mentioned that the newest challenge you face was the attacks on the public computer networks. If you will give us some examples of that, tell us why it is a problem, and then tell us what the solution is.

Mr. STEVENS. Yes, Mr. Chairman. What we have established in New York, and what we feel that will be the answer to this model, on the publicly owned or, if you will, government owned computer systems, will be a cooperative effort between the Office for Technology as well as the New York State Police, with advisory Committees from each one of the State organizations, with a rapid response team as well as teams that would be set up that would be able to manage their own computer systems, so that they could see that attacks were coming in and they could see if this attack was in fact being escalated to the point that it was an accidental probe or some intentional probe, where it may be compromising the system, and this may necessitate the need for investigative specialists and law enforcement then to go and pursue this investigation.

Mr. SMITH. What legislation, if any, would you like to see Congress pass to address that?

Mr. STEVENS. I am not sure if I know what legislation it would be, sir, but support in our efforts as well as financial support.

Mr. SMITH. I was just going to say more resources, more personnel, probably.

Mr. STEVENS. More resources and more personnel, for sure.

Mr. SMITH. We hope to have that coming with a bill passed at the very end of last year that supplied $25 million for cyber crime efforts. That has not been appropriated yet. So we hope to get some money toward some of those efforts.

Mr. McCaul, in your testimony you mentioned the rapid growth of cyber crime in Texas, and you specifically singled out child pornography. You were nice enough last week to tell me examples of how you all had apprehended those engaged in that trade in Texas.

I am wondering if you consider that to be the most serious type of cyber crime you face. You mentioned, for example, that one out of five children today are confronted with unwanted pornography over the Internet. Or is there some other type of cyber crime that you think we need to address? And also, if you will, tell all of us what you mentioned to me last week about any changes in legislation you think would be helpful to you.

Mr. MCCAUL. Yes. I believe that in terms of prioritizing these crimes, and there are so many of them, that the first and foremost one is to protect the kids and the children who are most vulnerable over the Internet, and so that is what my boss, the Attorney General, has mandated me to do, and that is what we have effectively done. It is so pervasive out there, and it is relatively untapped or unenforced, that it is frightening.

We have made a dent in that through partnerships like the Internet Crimes Against Children Task Force that we have with the Dallas police, but I think a model that has already been presented, that seems to work, that I think I would like to see go nationwide, and it is something that others have referred to, are these computer, regional computer forensics labs. The first one started in San Diego, and it is truly a joint State, local, Federal initiative.

In this area you have to combine the forces of government. You can't do it alone. And I would like to see, you know, we have done that in Dallas. You know, in Texas we have a regional lab, and it just opened a few months ago. It is working extremely well. This is something I would like to see go across the country, that I think could truly make a dent in attacking cyber crime.

Funding takes us to the next issue, that the Dallas office needs more funding. And I do believe with the act that I referred to you earlier, the funding was authorized and provided for. It just hasn't been appropriated. I believe with that funding we could truly bring our law enforcement efforts up to speed.

Mr. SMITH. Okay. Thank you, Mr. McCaul.

Mr. Cassilly, let me address my last question to you and ask you why you called cyber crime an epidemic in your testimony, And also, and perhaps from the point of view of the DAs, you might have some specific suggestions for legislative changes.

Mr. CASSILLY. Well, an epidemic, I mean, right now I am working with the National District Attorneys Association. We are having a summer conference which is completely focused on cyber crime. Everywhere I go, people are looking for training. They are trying to find, "Where can I go to learn about this?" It is very difficult, I mean, for prosecutors especially, because a lot of us are in small, two and three, four-man offices. and to have to go away for a long period of time impacts the office, so they are looking for the training to be easily available and accessible.

To give you an example of the impact of cyber crime on a local DA's office, Loudoun County, Virginia is the corporate headquarters for AOL. Loudoun County is about 200,000 people. I talked with the Commonwealth Attorney for Loudoun County, Virginia, and he told me probably a day doesn't go by where they don't get a request from prosecutors from New York to California, to help them to prepare search warrants or to prepare petitions for court orders to serve on AOL to obtain evidence.

And so what you have is the taxpayers of Loudoun County, Virginia supporting the nationwide war on cyber crime. That is the type of thing that the Federal Government should become involved in by going to the Justice Department, the U.S. Attorneys Offices and saying, "Hey, you guys should be the ones out there giving this assistance to the local prosecutors who are trying to pursue these

people across State lines." Without that help, it is very, very difficult.

We recently had a school shooting threat by cyber crime. We couldn't get the information from the ISP because they were closed for the night until after the school opened the next morning. So you had a school opening surrounded by armed police officers, and finally we managed to intercept, you know, get the information and do it. But it is the distance that is involved that really troubles, I think, a lot of local prosecutors in dealing with this.

Mr. SMITH. Thank you, Mr. Cassilly.

The gentleman from Virginia is recognized for his questions.

Mr. SCOTT. Thank you. I would like to ask the witnesses some jurisdictional questions, because this is one of the challenges with cyber crimes. Generally, you catch someone within your jurisdiction, a search warrant is issued for information that is physically within the jurisdiction, and some of the challenges that cyber crimes might have.

Mr. Cassilly, you indicated that if someone wants to subpoena evidence from AOL, they have to go to Loudoun County?

Mr. CASSILLY. Well, AOL will accept certain types of subpoenas directly from my office. For example, I can fax a subpoena. But under the Electronic Privacy Act, the Federal act, you can get certain information by way of a subpoena but if you want to go beyond that information, you have to get a search warrant or you have to get a court order. Those two documents have to be issued by a judge with jurisdiction specifically over AOL, so we have to go to Loudoun County for that sort of thing.

Mr. SCOTT. A subpoena, you just ask for the information. You don't have to ask permission to issue a subpoena?

Mr. CASSILLY. I guess I should clarify. AOL is good enough to accept our subpoenas without requiring us. Other ISPs actually require us to go through the local prosecutor to get a local subpoena. But AOL is trying to be as cooperative as they can be.

Mr. SCOTT. What standard do you need to issue a subpoena?

Mr. CASSILLY. Really, just a reasonable basis that there is criminal activity. But the evidence that you can get by a subpoena is very limited, also. All you can get really is the name, address, phone number, that sort of thing. If you want to go beyond that initial information, you have to get search warrants, which you are now moving into the area of probable cause.

Mr. SCOTT. And if a crime is being committed in cyber space, how do you know where it is being committed?

Mr. CASSILLY. You are asking—I go to the computer guys and I say, "Guys, figure out where this is being committed."

Mr. MCCAUL. I think the first step, you have to go—and I am not the expert either, but you have to—AOL is one of the few ISPs that actually will accept our subpoenas. A lot of them don't. Having a Federal law that would require them to accept State subpoenas would be helpful. But you have to go to the ISPs to get the subscriber identifying information, to find out——

Mr. SCOTT. Well, let's just give some examples. Somebody is in—a North Carolina prosecutor thinks a crime is going on in Raleigh, North Carolina. The ISP is AOL, and you need some information. How does the local prosecutor in Raleigh—what do they do?

Mr. STEVENS. If I might assist you, Mr. Scott, if we take the Raleigh case, it is probably very similar to New York. But we have to think about AOL as being one of the largest, and let's even think, let's go one step further. AOL really is not the Internet. AOL is the largest network, computer network, potentially, in the world, without going one step beyond to the outside world, being the Internet.

But within their own network, if you will, in New York State what we would need to do, it would be a grand jury subpoena, and we often have to go—we have to go before a grand jury to initiate an investigation. A subpoena would be issued to provide you with the information as to who the subscriber would be relative to that screen name that you may have, that you suspect in your case, and the only thing that is going to give you, Mr. Scott, the subscriber information, the name, the address where they live. That just starts your initial investigation.

Mr. SCOTT. How long does it take you to get that information?

Mr. STEVENS. Sometimes it may take up to a week or 2 weeks. In the case of online, let's say an online threat to a suicide, where someone calls you up and there is an online threat to a suicide, often this will take you several hours to get this information. There is a mechanism with AOL, and AOL works very well with law enforcement.

But now you have a suspect, or not a suspect, you have a potential victim online that is threatening suicide. And what we have to do is send a letter and prove to them that we have a police emergency here, and they will fax you forms to fill out and then you fax it back to them. And then you will get the subscriber information, which may not even be within your State, it may not be within your Nation, to get law enforcement within that jurisdiction to go and see if this person is at home.

Mr. SCOTT. How should it work?

Mr. STEVENS. I believe that, as my colleagues here have stated, we need subpoena power within our own States that will get us the Federal type of information that is needed. If we have an Internet service provider in California and there is no point of presence in New York, I am not sure that a New York subpoena works, sir. I am certainly not a lawyer. I am law enforcement. But I am not sure a New York subpoena would work in another jurisdiction.

Mr. MCCAUL. Yes, it depends on the ISP, whether they want to accept that subpoena out of State. If the ISP is out-of-State yet the victim, the victimization is occurring in Texas, for instance, where I am, that would be a nice standard to have under Federal law, that the ISP should accept service of process for that subpoena, and that that subpoena can be enforced. Because through that ISP there are illegal acts occurring in the State where the subpoena is originating.

Mr. CASSILLY. I mean, I think, Mr. Scott, your concern is, you don't want unnecessary or frivolous subpoenas being served to collect information. You have a privacy concern, which I understand. But I think that if the Federal law——

Mr. SCOTT. It is also a jurisdictional thing. If everything is going on in Virginia, a Kansas prosecutor can't be issuing subpoenas.

Mr. CASSILLY. Well, if there is a Federal—I mean, what I think would work is a Federal statute, if you want to put on that statute certain standards or requirements for certain information to be met, but the point being that if the Kansas prosecutor is dealing with the school bomb threat or the school shooting threat, and they don't have lots of time to go through, back and forth, and getting a prosecutor in another State to get a judge out of bed to, you know, sign something, and then hand-carry that down to the ISP or somebody.

So, I mean, I can understand the privacy concerns, and if there was Federal legislation, you could require certain findings or certain information be contained in the subpoena. The ISP could satisfy itself that, yes, there is legitimate need for this information, but they would then respond to that subpoena.

I mean, the only people that are concerned with jurisdictional issues are the local prosecutors and the local police. The ISPs don't know anything about jurisdiction. They are—you know, AOL could have somebody sending messages from England through AOL to California or something, and the only thing that is in Virginia is simply an electronic pass-through and a large computer that tracks Internet addresses and Internet information.

Mr. SCOTT. Thank you.

Mr. SMITH. Thank you, Mr. Scott.

The gentleman from Wisconsin, Mr. Green, is recognized for his questions.

Mr. GREEN. Thank you, Mr. Chairman.

Well, obviously the questions that Mr. Scott is asking really touch upon the crux of the matter and the challenges we have to deal with.

Mr. Cassilly, in the same area of your testimony in which you talk about these very issues, you also say that Federal laws should make it possible for Federal law enforcement and U.S. Attorneys to use their offices to assist in the preparation of subpoenas and warrants and the service of same. If you would go into some more detail on that, how the U.S. Attorney's Office could be helpful to you.

Mr. CASSILLY. Well, one of the ways they could be helpful is by designating, predesignating specific local prosecutors as Assistant U.S. Attorneys, and allowing them to prepare subpoenas or search warrants and go to the Federal court as cross-designated Assistant U.S. Attorneys, and have Federal warrants or Federal court orders issued which are then transmitted to the ISP or the record storage facility, so that the standard that is being used is the standard that would be applied by a Federal judge to do this sort of thing.

That gets a little scary, because I know that there aren't any Federal judges out there that are just sitting around with nothing to do, so I mean, that becomes somewhat of a problem in terms of the total numbers of these things that are coming in. That is why it seems to me that the more practical—I mean, you could reserve that for search warrants, reserve that for court orders only, and have just the informational subpoenas, have a Federal requirement that the ISPs submit or accept and honor subpoenas for the bare identifying information from wherever they were received.

Mr. GREEN. Would we then have to, in our Federal law, specify the uniformity of those warrants, so that you have got the ISP not receiving conflicting warrants or all different kinds of requests?

Mr. CASSILLY. It seems to me that that would be reasonable from the ISP's standpoint. It would also cut back in delay. If the prosecutor knew what was required and could put that information in up front, then they wouldn't waste time with sending a subpoena to an ISP only to have it bounce back because their legal department says this isn't a good subpoena. So I think it would benefit both sides to have very specified information that was required.

Mr. GREEN. So the first step would be to federally provide for this type of service; then, secondly, a massive educational effort in reaching out to every State's prosecutor throughout the Country and saying, "This is available. This is how it's done."

Mr. CASSILLY. I can assure that the National District Attorneys Association would be more than happy to make a national educational effort to do that, to convey that information.

Mr. GREEN. Interesting. I have no more questions, Mr. Chairman.

Mr. SMITH. Thank you, Mr. Green.

The gentlewoman from Houston is recognized for her questions. Although Mr. Delahunt, I could tell, was ready and able. May we go to Mr. Delahunt?

Ms. JACKSON LEE. That is fine, Mr. Chairman.

Mr. SMITH. Okay. The gentleman from Massachusetts is recognized for his questions.

Mr. DELAHUNT. I don't mind waiting.

Mr. SMITH. Mr. Delahunt, let me explain. As you know, the full Chairman is happy just to recognize people in the order they arrived, and that is supposedly the way we need to have our Subcommittees run, as well. And since you were here first, I thought the gentlewoman from Texas wouldn't mind yielding to you.

Mr. DELAHUNT. Well, I will do whatever you wish, Mr. Chairman, but if you want to establish a different set of standards than the full Chair in the Committee, I won't squeal. I will keep it between us.

Mr. SMITH. I think we will recognize the gentleman from Massachusetts for his questions.

Mr. DELAHUNT. I appreciate the problems that you have articulated. Before I make this comment, I want to preface it by saying that I was an elected State's prosecutor for 21 years myself. But I think if the problems that you—and I think we should address them along the lines that you have suggested.

At the same time, I presume in most cases there will be, if there is a violation of a State statute, there is a corresponding substantive violation of the United States Code, so that a call to the United States Attorney's Office outlining the problem and deferring to the United States Attorney is one—I see Mr. Cassilly is really ready to respond to this—would be an approach that could be taken.

Mr. CASSILLY. I will bite my tongue.

Mr. DELAHUNT. But I—and I do, by the way, share that same concern—but I mean, there are ways to deal with it. But I think

it is important, honestly, that we do empower State and local jurisdictions also.

Mr. CASSILLY. I mean, my sense about going to the U.S. Attorney's Office is that I recently took a child pornography case to the U.S. Attorney's Office because the Federal law on child pornography was better than the Maryland statute on child pornography, one; two, the case, the computer evidence had been in the lab for so much time that the statute of limitations on the misdemeanor charges in Maryland had run already, and I could not get the U.S. Attorney's Office to not only take the case, but you know, even give me a reason for not taking the case, so——

Mr. DELAHUNT. They declined jurisdiction?

Mr. CASSILLY. They declined the case, and it was a child pornography case, which I was appalled that that wasn't something that they would grab onto. So, I mean, given the number of prosecutors around, local prosecutors around the Country, I don't think that the U.S. Attorneys are going to be lining up to take our cases or consider most of this stuff. A lot of the attitude is—and I think, for example, computer fraud, many, many, many computer frauds are way under the guideline cutoffs that the U.S. Attorneys use. You couldn't get them to touch it.

Mr. DELAHUNT. What are the guidelines, in terms of is it a $10,000 standard——

Mr. CASSILLY. My U.S. Attorney is using $100,000.

Mr. DELAHUNT. $100,000?

Mr. CASSILLY. Right, and a lot of computer frauds are much less than that. If you don't deal with them, the guy is just encouraged to keep doing it again and again.

Mr. DELAHUNT. Right. No, again, I mean, but I think it is important that the panel be aware that there is jurisdiction out there, Federal jurisdiction that I would dare say in the vast majority of cases runs parallel to State and local jurisdiction in terms of the substantive crime itself, so that——

Mr. MCCAUL. If I could just add, two of our prosecutors are actually cross-designated to practice in the Western District and the Northern District of Texas, but typically we will make that determination early on, is this going to be a Federal or a State case——

Mr. DELAHUNT. Right.

Mr. MCCAUL [continuing]. Based on the threshold amount of money or, you know, the penalty provisions, Federal versus State. But I agree, I think, yes, there are certainly some State offenses that may not be Federal, and vice versa, and you need to respect those differences.

Mr. DELAHUNT. Is the NDAA and NAAG and other groups, are you working on any kind of model legislation? I mean, this is clearly just a hearing, and I think that you can infer from the questions that are being asked, you know, how should it work, that it might be well worth the time and effort to begin drafting some concrete proposals in terms of legislation for Congress to consider.

I mean, I can understand the jurisdictional issues. I also think that in a forensic—you know, you said computer laboratories out in San Diego—I would even expand it. I always, in high profile cases or serious cases, it was always an inclination on the part of local or State prosecutors to utilize the FBI lab, and we all know

there is a long wait there, and there have obviously been problems there. But the concept of a forensic laboratory I think is something that is, on a regional basis, that would be readily available for local, State law enforcement, just makes an awful lot of sense, particularly now with the issue of cyber crime.

Mr. MCCAUL. It is a great training mechanism, too, because the FBI initially operates those labs. They can train law enforcement and then turn it over to the local people.

Mr. DELAHUNT. But having NAAG and NDAA working with the Department of Justice, too, to establish standards, I mean that can be done in a working group environment.

Mr. MCCAUL. And NAAG has highlighted the issue of the jurisdictional disputes and boundaries. I think they are paying close attention. I think that is an excellent idea, that they could take a stab at drafting something.

Mr. CASSILLY. It would be done a lot better, too, if there was some financial assistance or incentive for some more regional cooperation, too. I mean, it is really interesting that the San Diego regional forensic lab has police officers working in the lab from 27 different jurisdictions. I mean, I challenge anybody to find anything similar to that anywhere in this country.

Mr. DELAHUNT. That is good.

Mr. SMITH. Thank you, Mr. Cassilly.

The gentleman from Virginia, Mr. Goodlatte, is recognized.

Mr. GOODLATTE. Thank you, Mr. Chairman, and I want to thank you and commend you for holding this hearing on a subject that is of great interest to me. As Chairman of the Congressional Internet Caucus, I see all of the great wonders of the Internet, its uses for education, for conducting business, for communications. It is really, now and in ways that we can't even foresee, revolutionizing the way we live.

But it has on it virtually all of the seamier sides of life, as well, and while not every type of crime that is committed off of the Internet is committed on the Internet, a great many of them are, of all degrees of magnitude and all types, and that requires a great deal of work by local law enforcement to handle those things. It cannot be handled entirely by the Federal Government, by any stretch of the imagination.

But, by the same token, it creates a whole set of new challenges for local law enforcement, both from the standpoint of training and from the standpoint of doing work, as Mr. Cassilly pointed out, that really is benefitting somebody in a whole different part of the country in terms of fighting crime, but the burden gets spread around.

In my part of Virginia we have a local sheriff's department that is very, very dedicated to this, has been for the past several years, called Operation Blue Ridge Thunder, the Bedford County Sheriff's Department, that operates originally under a grant from the U.S. Department of Justice's Office of Juvenile Justice and Delinquency Prevention. And they have referred people for arrest in literally dozens of jurisdictions around the country, that they have in their task force and their sting operations and so on uncovered people attempting to communicate with children and others in their area.

So having Federal Government support to help lift this burden I think is very important, and I think this discussion about pos-

sibly looking into ways to facilitate the recognition and action on subpoenas that go across State lines might be something that this Committee could very well work on.

I would like to ask each of these three witnesses if they have participated in the pilot projects that I have referred to. It started out with 10 cities and counties around the country. I think they have expanded that to 20. They are now attempting to give smaller grants to more law enforcement agencies, and they are trying to use the ones that have the larger grants to be sort of a training ground and a source of assistance for other local law enforcement agencies in their particular States.

Mr. Stevens?

Mr. STEVENS. Yes, sir. If I may address that, as a matter of fact, we have cooperated with the Blue Ridge Thunder, some of their investigations. We were one of the first 10 grant recipients in this Internet Crimes Against Children's Task Force, and we have heard how important this is protecting our most valuable asset, our children. As a matter of fact, the case that we worked with, I had 5 seconds of glory on 48 Hours, I believe.

But that is a unique model. It is a model that is being funded by the Federal Government, giving local and State law enforcement agencies Federal tools to work with. It is a unified, systematic program where they are trained, where we are trained, and though we have mentioned jurisdictional issues here, we found a way to bridge these jurisdictional issues by all working off the same model.

For instance, in Blue Ridge Thunder's case, they provided us with our probable cause, and we made application and got a search warrant and waited at the airport for this predator to show up.

Mr. GOODLATTE. Along with the 48 Hours crew, I might add.

Mr. STEVENS. Yes, sir. Yes, sir. But it is a great model. That needs support. That is a great——

Mr. GOODLATTE. Does it need more funding? Would it be a recommendation of you that the Congress put more money into this program and empower more local law enforcement to——

Mr. STEVENS. Yes, sir. What I strongly suggest is that each State has a model like this, at least one point of contact in that model. There are satellite grants that are issued. Satellite grants are a much smaller amount. But this is a great tool. It is a great tool for all of us, to protect our children, our grandchildren.

Mr. GOODLATTE. Let me ask you, what I found in this area—and we had a demonstration here on Capitol Hill through the Internet Caucus a couple of years ago, of the types of these crimes that occur on the Internet, and it is truly, I think, astounding to most Members when they first see—Mr. Chairman, I think you had the opportunity to see some of these types of absolutely the most hardcore pornography, victimizing hundreds of thousands of children, and they make these initial contacts in chat rooms.

And I find that Operation Blue Ridge Thunder and probably your organization focuses on the ones who actually then become what are referred to as travelers, and go to other jurisdictions to try to meet with these children. But cutting them off at the pass, when they engage in these initial, highly explicit sexual discussions with

minors on the Internet, have you any experience in attempting to prosecute people for that initial contact?

If we could make those chat rooms safer for children, both in terms of educating them, keeping them away from them, but also in terms of prosecuting people who attempt to engage in that type of sexual discussion with minors, I don't know where the constitutional line is, but I think it ought to be tested and we ought to find out whether there is a way to put a chilling effect on that very type of behavior.

Mr. STEVENS. Many times, sir, what happens is you have to continue these chats, because technology crime is no different than any other crime, but it is often you have to be able to place someone at that keyboard. Who is that person, that person you can't see?

And I often use the analogy that "she" can be a "he" and 13 can be 30 on the Internet. No one knows who is at the other end of that monitor and who is chatting with you, and often you have to continue to communicate so that you can figure out who that is. And there may be problems with some of the laws, that you may only have an attempt to commit a crime at that point because they haven't made that overt act. But legislation certainly could be drafted, and——

Mr. GOODLATTE. Well, we want some guidance on that. Before we jump out and challenge the Constitution, we want to make sure we think we are on the right side.

Mr. MCCAUL. On undercover work, one case I illustrated in my opening statement, in these chat rooms, the Internet Crimes Against Children Task Force, they work very closely with us on these cases. When the actual solicitation is made online, we typically tend to follow it through with a meeting, say at a hotel room or something to that effect, so you do have the overt act and it is a predisposition, you know, he is predisposed.

Mr. GOODLATTE. I agree with that, but the problem there is, that sends the message to the person engaged in this type of activity that as long as they keep it on the Internet, it is okay to do it, and it is only when they attempt to try to have a face-to-face meeting with the child, are they at risk. And if we could have a reach into those chat rooms and have some enforcement mechanism to put a stop to this, there are literally hundreds of thousands of those conversations going on right now, as we sit here, and it is an amazing phenomenon and a very dangerous one, too.

Mr. STEVENS. Anyone can create a chat room. Anyone can name it anything they want. Whether they are going to get someone to chat with them, that is another story, but——

Mr. GOODLATTE. I don't want to discourage you from going after the ones that are—we arrested one in Bedford County who had a machete and a baseball bat in the back seat of his car, and who thought he was meeting with a 14-year-old girl and had come up from North Carolina. They prosecuted a former chief of staff to the Governor of West Virginia. I mean, they have had great success in doing those things, but we need to take it a step further. We need to figure out a way to do that constitutionally and effectively.

Mr. SMITH. Thank you, Mr. Goodlatte.

The gentlewoman from Texas, Ms. Jackson Lee, is recognized for her questions.

[The prepared statement of Ms. Jackson Lee follows:]

PREPARED STATEMENT OF THE HONORABLE SHEILA JACKSON LEE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Thank you Mr. Chairman.

Mr. Chairman, all Americans have a vested interest in balancing the policing of cyber crimes with the protections, of civil liberties and speech on the internet. Finding the right balance is crucial.

Last year this Subcommittee held a hearing on the series of well-planned and coordinated cyber attacks on several of the nation's biggest Internet sites. Two popular sites, Yahoo.com. and Buy.com, were shut down for several hours, while cites such as CNN.com, ZDNet.com, Amazon.corn, eBay.com, and E*Trade were similarly terrorized. These cyber attacks effected millions of Internet users and resulted in revenue losses for several sites. While this damage was relatively minimal in proportion to volume of the internet, these events were a wake-up call to many of us as to the extent of cyber crime, and the degree to which we are all vulnerable.

The world of electronic communications is a developing one. Clearly, there is a growing need for enforcement, and in many instances, strengthening of our laws so that our law enforcement professionals can do their jobs and keep us all safe from cyber criminals.

Having said this, we must also recognize the need to heed the warnings from the examples of deprivations of civil liberties that are more and more abundant as the internet continues to grow, and law enforcement struggles to keep up.

In a recent case in the state of Texas which I represent, law enforcement acting on a tip from a local business, confiscated all of its competitor's business computers based on the accusation that the competitor engaged in electronic "spamming." As a result, the accused business, against which charges were eventually dropped, lost months of business while incurring legal and other costs to get its equipment back.

To balance enforcement with protections, there must be a concerted effort to coordinate law enforcement between federal, state and local entities. We must provide them with the equiptment and training to enable them to keep up with the criminals who are operating in the cyber environment. In the process, we must protect the rights of Americans to free political, commercial, and other speech over the Internet.

To this end we have many challenges. We need a balanced international strategy for combating cybercrime. We need round-the-clock federal, state and local law enforcement officials with expertise in, and responsibility for, investigating and prosecuting cybercrime. We need new and more expansive procedural tools to allow state authorities to more easily gather evidence located outside their jurisdictions, and need to assess whether we have adequate tools at the federal level to effectively investigate cybercrime. We need to work in partnership with industry to address cybercrime and security, where we can discuss challenges and develop effective solutions that do not pose a threat to individual privacy. Finally, we need to teach our young people about the responsible use of the Internet.

It is the role of government to protect all of these forms of speech, as well as interstate commerce that over the Internet. To this end, we must send a clear message to those who would attempt to interfere with the free speech and mobility of citizens and industry through the internet—Americans take this very seriously. Cyber criminals will be dealt with as are all other criminals.

I look forward to your comments.

Ms. JACKSON LEE. I thank the witnesses very much for your presentation, and I have had the opportunity to peruse your written statements, and so I am going to raise some of the questions and concerns even though I did not get to hear all of your testimony. And I welcome you, Mr. McCaul. You are based in Austin?

Mr. MCCAUL. Yes, ma'am.

Ms. JACKSON LEE. I welcome you and thank you for the very special work that the State of Texas is doing on these issues. I think if there is something that the Federal Government has, it is the bully pulpit, if you will, and I hesitate to use the word "bully" because we are in another date, another time, yesterday, trying to di-

minish bullying in the school yard. But I do think that the Federal Government has that privilege because the Internet, although it is personal and private, it is viewed as a national entity. Just the very sound of its name suggests that it flows throughout the country, and of course throughout the world.

And with that in mind, I would like—I noted, Mr. Stevens, the list of legislative initiatives—but I would like us to just be creative and imagine what other roles the Federal Government could take in this. And I appreciate Mr. McCaul's comment that not one level of government is the answer. It is an integrated process.

So let me ask a general question, but let me be pointed in my questioning. First of all, we know that the criminal prosecution or the ability to charge persons unfairly crosses all technologies. You can go down to the Justice of the Peace court and file against your neighbor wrongly. But I cite the case in Texas, the business case where a business was accused of spamming, and of course all records were seized, and it proved I guess to be a false case.

I would like to distinguish that because in that instance it is a business issue. It doesn't seem to have any life or death questions, except of course a business person certainly doesn't like being put out of business. But when we deal with children, I think we can raise the ante, because besides the chat room, I think the most horrific final results of the predator is to solicit that child from the safety of their home, their family, their neighborhood, their community, to leave that home and possibly never to be found again.

We have certainly had some stories where we have discovered the criminal act, but we don't know if we have had those that we have not discovered. Solicitation after the child has been brutalized psychologically and feels that this is a place that they should go, and maybe ultimately winding up in a loss of life of that child.

I would like Mr. McCaul to walk me through the case that you cited regarding a 25-year-old school teacher, how your Internet Bureau actually was able to intercede, permeate this particular situation. Were you called in by the police on the ground, or did your Internet Bureau first discover this particular——

Mr. MCCAUL. I believe that was a case that originated out of the Internet Crimes Against Children's Task Force, and there is a—some of this is sort of sensitive in terms of techniques in undercover operations, so I am a little hesitant to get into specifics in that respect, but the suspect was clearly predisposed to this type of behavior and then went into this chat room and solicited sex. We had an undercover officer, obviously, on the other end, where there were conversations online about meeting in the hotel room and having sex.

He showed up to a—this is a school teacher, which is to me frightening—he showed up to a hotel room in Austin, Texas, and was met with the Austin police and our peace officers. He showed up with pornographic materials and various other sundries I would rather not get into.

Ms. JACKSON LEE. His prototype, then, was made prior to. You knew that he fit the—he had been sort of made beforehand——

Mr. MCCAUL. That is correct.

Ms. JACKSON LEE [continuing]. And you were able to intercept him and do the work through the Internet Bureau.

Mr. MCCAUL. As you know, if they are not predisposed, then you have entrapment issues. He was clearly predisposed at that point in time. And then we discovered, frighteningly, that he had also—that he had already raped a 15-year-old in Waco, Texas, and so he is facing charges on that.

Ms. JACKSON LEE. Let me ask all three of you now the question I would like to pose, and I think I asked sort of the broad question, what the Federal Government can do. I think that there is always a higher standard for criminal acts, but here we have a situation where it is very hard to get our hands around it.

But in relation to the Internet and technology, can we strike a balance dealing with the respect for privacy and civil liberties, and can we strike a balance with how we do property crimes? My concern, if a hacker, a teenager, a 15-year-old is fooling around and causes property loss, dollars, should I be so punitive and so final on his penalties versus those that are engaged in these heinous acts dealing with our children? Because that is where you get the radar screen. That is where people begin to be horrified. Can we manage to find some balance in that? Have we done so in the law generally? Mr. Stevens?

Mr. STEVENS. If I might answer that, I have been involved in technology crime for the past 10 years, and when we first got started, my previous—the division of work I was doing prior to this was undercover narcotics. When I came into this field, I was very sensitive and still am extremely sensitive to privacy issues. And I have 26 years with a police department, with the New York State Police, and the last thing that I want to do is violate anyone's civil rights or violate anyone's rights or privileges.

And I have encountered several different cases, one of which was a bomber. He actually created a bomb, but he was a journalist as well, so his writings were protected by law. The judge issued an order. I made application for a search warrant, and a search warrant was authorized. I couldn't visually examine his computer, but I could create a search string to search for any bombs, nitrates, any word I could come up with that referred to bombs and things of that nature, thereby protecting his journalistic respect.

Properly trained law enforcement officers, with training relative to legal issues, is the answer. And training is a big resource that we all need, we all need at the State government and at local government. That is a real big issue.

Mr. SMITH. Mr. Stevens, I have heard of journalists throwing verbal bombs but not material bombs. That is interesting.

Ms. JACKSON LEE. May I let Mr. McCaul and Mr. Cassilly answer that sort of broad question?

Mr. SMITH. If you all will respond to the question, please. Thanks.

Mr. MCCAUL. I'm sorry. Could you repeat the question?

Ms. JACKSON LEE. The balance between civil rights, civil liberties, and property crimes, and crimes of sex against children, how do you find the balance?

Mr. MCCAUL. Yes, I think you obviously respect civil rights. I think that in our office we have, as I mentioned earlier, prioritized these crimes. You cannot—unfortunately, it is so pervasive, you cannot attack every one. We have prioritized these, first and fore-

most protecting the kids, as I said, the child pornography type cases, child predator type cases.

And with respect to a crime of property versus child pornography or a more violent act over the Internet, I think most prosecutors would lean toward the more violent act. But you are really in an area of prosecutorial discretion, and in our State, as you know, there are district attorneys all across the State and they have discretion to do what they want to do. But I will say that most of them do the right thing, and I think they put crimes of violence at the top.

Ms. JACKSON LEE. Thank you.

Mr. CASSILLY. I think one of the points, too, is that property crimes probably for the most part go unreported. I recently attended a workshop with private investigators in the cyber crime area. These are people that are hired by large corporations and businesses to investigate attacks on their computer systems and theft of their intellectual property. And one of the points made by the private investigator was that, for the most part, these folks don't want them going to law enforcement once they have solved the cases, because they don't want to attract the publicity, they don't want this sort of stuff known.

The other problem with property crimes is, they are much more difficult to prosecute. I recently had a complaint from eBay, where eBay had tracked back to my county a solicitation where some guy was selling some collector's item for $35 apiece, and eBay had something like 100 complaints from all over the Nation where this guy had taken people's $35 and hadn't sent them anything. They wanted to know if I would prosecute, and I said, "Well, where are the victims?" Well, the victims were—there wasn't a single victim inside the State of Maryland. I am not spending $300 a victim to fly them in to testify about a $35 theft, even though the cumulative value was $3,500. So basically the guy got away with a crime.

I think that for most of us, as a local prosecutor, I don't need to go looking for work, and if there is anything that is shady or close to the line or something, I just throw it on the shelf and go to the next thing that is more up front and easier to prove, and just is that much more simple and direct as far as the case I have got.

Ms. JACKSON LEE. Thank you, Mr. Chairman.

I just, Mr. Cassilly, since you are close to this, being the people's lawyer, would that mean for example trying to deal reasonably with a 15-year-old that is doing the property crime? You know, the concern is, our children are sophisticated on one end, meaning that they are expert computer users or have knowledge, that they might be one of those offenders, those hackers, etcetera. Do we round them up and throw them in jail?

Mr. CASSILLY. In my State system, and this is probably peculiar to Maryland, I am not aware of the other States, but before the prosecutor even gets to the juvenile, the juvenile is referred to the juvenile services folks who determine whether counseling is appropriate, look at the background, look at the availability of a whole bunch of other resources. It is only in the event that they can't work out anything with the kid and his parents, that the prosecutor becomes involved.

Ms. JACKSON LEE. Thank you.

Mr. SMITH. Thank you, Mr. Cassilly.

Thank you all, and let me say that we have learned a lot today, both about standardization, about jurisdiction, about subpoenas, and the need for additional resources for both training and prosecution, so it has been very helpful to us. We appreciate your testimony, and frankly will look forward to your continued good advice, and the Subcommittee stands adjourned.

[Whereupon, at 2:55 p.m., the Subcommittee was adjourned.]

FIGHTING CYBER CRIME: EFFORTS BY FEDERAL LAW ENFORCEMENT

TUESDAY, JUNE 12, 2001

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CRIME,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 4 p.m., in Room 2237, Rayburn House Office Building, Hon. Lamar Smith [Chairman of the Subcommittee] presiding.

Mr. SMITH. The Subcommittee on Crime will come to order. We welcome all the witnesses today. We look forward to your testimony. As you know, this is an important subject, a subject and a hearing that is going to give us ideas for future legislation. I'm going to recognize myself for an opening statement and other Members for an opening statement, and then we will proceed with your testimony.

This is the Crime Subcommittee's second of three hearings on cyber crime. Today we will hear testimony from the Criminal Division of the Department of Justice, the Federal Bureau of Investigation and the U.S. Secret Service on the role and needs of Federal law-enforcement in this effort. In addition, we will hear from the Center for Democracy and Technology, CDT, about online privacy concerns related to law-enforcement efforts to protect the public.

The growth of the Internet has improved our economy, medicine and technology. Unfortunately, it has brought new opportunities for criminal activity, as well. Often, people think cyber crime simply refers to hacking, viruses and other intrusion tactics. Cyber crime, however, threatens more than our businesses, economy or national infrastructure. Cyber crime affects us individuals, as well. Reprehensible crimes, such as child pornography and cyber stalking, terrorize our children and our families.

At the first hearing in this series, on May 24th, the Texas Deputy Attorney General for Criminal Justice testified that, quote, "One of the biggest problems is that computer criminals are targeting the most vulnerable of our society, children." He pointed out that, according to the Federal Bureau of Investigation, child pornography was virtually extinct prior to the advent of the Internet. Now it is a serious plague on our society that must be stopped.

Adults also experience the dark side of the Internet revolution. Using computer technology, criminal types steal life savings and even identities of unsuspecting individuals. These pose serious threats to the lives and the livelihoods of many individuals. But in addressing these areas of crime, law-enforcement officers face sev-

eral challenges. Identifying a sophisticated criminal can be difficult. Once they are identified, bringing a criminal to justice may be problematic for jurisdictional reasons.

The criminal may be in a different State or even another country, and then law enforcement officials must deal with extradition issues. Also, retrieving the information stored on a computer and using it for prosecution may be difficult if it requires highly technical skills not normally taught to investigators or prosecutors. As long as there is technology, cyber crime will exist, yet cyber crime must be curtailed as much as possible so that technology can legitimately continue to enrich our lives and strengthen our economy.

Congress understands that law-enforcement officials must have the appropriate training and equipment to fight fire with fire, or computer technology with computer technology; but in doing so, law-enforcement must remain cognizant of the need to protect the law-abiding public's privacy while protecting the public. The public must understand that law-enforcement does need to use technology to deal with this new emerging threat to our children, our economy and our national security.

This hearing will focus on those efforts and challenges. We look forward to hearing how to balance the concerns of law-enforcement officials and the need to protect privacy and find common ground to fight the growing trend of cyber crime. Before I recognize Mr. Scott, the Ranking Member, for an opening statement, I would like to congratulate the FBI, the Department of Justice and the Secret Service on the successful Internet fraud investigation named Operation Cyber Law. Their efforts brought about criminal charges against approximately 90 individuals and companies that defrauded 56,000 people out of more than $117 million.

With that congratulations, I will now recognize Mr. Scott for his opening statement.

[The prepared statement of Mr. Smith follows:]

PREPARED STATEMENT OF THE HONORABLE LAMAR SMITH, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

This is the Crime Subcommittee's second of three hearings on cyber crime. Today, we will hear testimony from the Criminal Division of the Department of Justice, the Federal Bureau of Investigation and the U.S. Secret Service on the role and needs of federal law enforcement in this effort.

In addition, we will hear from the Center of Democracy and Technology (CDT) about on-line privacy concerns related to law enforcement efforts to protect the public.

The growth of the Internet has improved our economy, medicine and technology. Unfortunately, it has brought new opportunities for criminal activity, too. Often people think cyber crime simply refers to hacking, viruses and other intrusion tactics.

Cyber crime, however, threatens more than our businesses, economy or national infrastructure. Cyber crime affects us as individuals, too.

Reprehensible Crimes, such as child pornography and cyber stalking, terrorize our children and our families.

At the first hearing in this series on May 24th, the Texas Deputy Attorney General for Criminal Justice testified that "one of the biggest problems is that computer criminals are targeting the most vulnerable of our society—children." He pointed out that according to the Federal Bureau of Investigation, child pornography was virtually extinct prior to the advent of the Internet. Now it is a serious plague on our society that must be stopped.

Adults also experience the dark side of the Internet revolution. Using computer technology, criminal types steal life savings and even identities of unsuspecting individuals. These pose serious threats to the lives and the livelihoods of many individuals.

But in addressing these areas of crime, law enforcement faces several challenges.

Identifying a sophisticated criminal can be difficult. Once they are identified, bringing the criminal to justice may be problematic for jurisdictional reasons. The criminal may be in a different state or even another country and then law enforcement officials must deal with extradition issues.

Also, retrieving the information stored on a computer and using it for prosecution may be difficult if it requires highly technical skills not normally taught to investigators or prosecutors.

As long as there is technology, cyber crime will exist. Yet cyber crime must be curtailed as much as possible so that technology can legitimately continue to enrich our lives and strengthen our economy.

Congress understands that law enforcement officials must have the appropriate training and equipment to fight fire with fire, or computer technology with computer technology. But in doing so, law enforcement must remain cognizant of the need to protect the law-abiding public's privacy while protecting the public.

And the public must understand that law enforcement does need to use technology to deal with this new emerging threat to our children, our economy and our national security.

This hearing will focus on those efforts and challenges. We look forward to hearing how to balance the concerns of law enforcement officials and the need to protect privacy and find common ground to fight the growing trend of cyber crime.

Before I recognize Bobby Scott, the ranking Member, for an opening statement, I would like to congratulate the FBI, the Department of Justice, and the Secret Service on the successful Internet fraud investigation named "Operation Cyber Loss." Their efforts brought about criminal charges against approximately 90 individuals and companies that defrauded 56,000 people out of more than $117 million. With that, I recognize Mr. Scott.

Mr. SCOTT. Thank you. Mr. Chairman. I am pleased to join you in convening the second hearing on the issue of cyber crime. In the first hearing, we heard about State and local law-enforcement efforts to combat cyber crime. Today we will focus on Federal law-enforcement's efforts to combat cyber crime and we will hear from Federal agencies most involved in the issue, and one of our watchdog entities, working to ensure that we do not lose sight of our basic rights and protections as citizens in our zeal to address the menace posed by cyber crime.

Given the jurisdictional issues involved in crimes undertaken by way of electronic communications, the Federal Government will be in a better position to address such crimes in many instances and State and local law-enforcement entities. However, the nature of cyber crime remains the same despite the different medium: theft, fraud, forgery, destruction of property and so forth, violation of laws already on the books at State and local levels. So it is no surprise that we heard from State and local law-enforcement witnesses at the last hearing, that much of the role that they envision for the Federal Government in fighting cyber crime focuses on their need for resources, training, cooperation and assistance, not Federal usurpation of the enforcement effort.

Of course, in any case of criminal activity, including cases of cyber crime, we are all better off with the emphasis being placed on crime prevention, as opposed to placing it on after-the-fact solutions. Thus, identifying ways to prevent cyber crime through better system security, crime prevention education programs for users and businesses, and early detection of and attention to potential problems should provide our best defense to cyber crime.

The rapid advancements we're seeing in information technology in the context of the World Wide Web not only challenges our ability to enforce traditional criminal laws, but also challenges our ability to protect and enforce basic rights of privacy and the other

civil liberties our Constitution guarantees to us. Therefore, we should look at updating our law-enforcement capacities in this context, and it is just as incumbent upon us to make sure that these basic guarantees are not eviscerated or seriously compromised.

We must never lose sight of the fact that the enduring success of our system lies in the delicate balance our founding fathers struck in giving our Government strong authority to provide for the general welfare while protecting the sanctity of individual rights and the freedoms of law-abiding citizens from undue Government intrusion. It is interesting, Mr. Chairman, that we had a Supreme Court case just yesterday that addressed that issue. So, Mr. Chairman, I look forward to the testimony, to learn more about the challenges and activities of our primary law-enforcement Federal agencies in addressing the issue of cyber crime, as well as the challenges we face in preserving our civil liberties in the context of the World Wide Web.

Thank you, Mr. Chairman.

Mr. SMITH. Thank you, Mr. Scott.

Do any other Members wish to be recognized for an opening statement? The gentlemen from North Carolina, Mr. Coble, is recognized.

Mr. COBLE. Mr. Chairman, I will be very brief. I have no formalized statement, and I may have to go to another meeting; but Mr. Assistant Attorney General, I put this question to the Attorney General last week, when we examined him up here, and I'm repeating this just for emphasis. I am concerned about your updating the Subcommittee on the extent to which prosecution of intellectual property crimes is becoming or has become a priority for the Department of Justice, A, and, B, if you all are using the provisions of the NET Act to pursue cyber pirates, or is it just a dead law? I'm hoping not the latter—and what could we do to help in regard to these two matters?

If I am not here at the conclusion of your testimony, if you can touch on that, I would be appreciative.

Mr. CHERTOFF. I will do that.

Mr. COBLE. Thank you, Mr. Chairman.

Mr. SMITH. Thank you, Mr. Coble, and I will incorporate those in my questions, so we will have the answers for you in that regard. If no other Members wish to be recognized, we will go to our witnesses and I will introduce them. They are Mr. Michael Chertoff, Assistant Attorney General, Criminal Division, U.S. Department of Justice; Mr. Thomas A. Kubic, Deputy Assistant Director, Criminal Investigative Division, Federal Bureau of Investigation; James A. Savage, Jr., Deputy Special Agent in Charge, Financial Crimes Division, United States Secret Service; and Mr. Allen B. Davidson, Associate Director, Center for Democracy and Technology.

Again. we welcome you all, and Mr. Chertoff, if you will begin——

STATEMENT OF MICHAEL CHERTOFF, ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, U.S. DEPARTMENT OF JUSTICE

Mr. CHERTOFF. Thank you, Mr. Chairman. Mr. Chairman and Members of the Subcommittee, thank you for giving me this opportunity to testify about the Department of Justice's efforts to fight cyber crime or computer crime. Although I have been Assistant Attorney General for the Criminal Division for only little more than a week, it is clear to me already that this issue being considered by the Committee today is one of singular importance, and I commend the Committee for holding this hearing.

Let me give you a few real world examples of what we face with the cyber crime problem. These are drawn from real cases. A woman places a notice or appears to place a notice on the Internet that says, quote, "It is my fantasy to be raped. Here is my name, home address and telephone number." In fact, this posting was not sent by the woman, but by a man who wanted to punish or harass the woman for some personal spurning of his romantic advances. Over the next few weeks, six strangers knock on her door in the middle of the night, attempting to respond to the posting. Luckily, the woman manages to convince them that the Internet notices were hoaxes.

I will give you another example. A virus is released in a foreign country. Within days, it has disrupted the communications of hundreds of thousands of computers across the Internet, causing losses estimated in the billions of dollars. The virus is designed so that after it infects a computer, it will access the user's computer passwords and relay them electronically back to the foreign country.

A third example, an organized group of hackers from Russia and Eastern Europe commit a series of intrusions into more than 40 banks and e-commerce companies in the United States. The hackers steal over one million credit card numbers from the company's databases and then sell them to organized crime. The hackers then extort the companies, threatening to disclose their confidential information or damage their computer systems.

These scenarios are not alarmist speculation. They are based on actual events and cases, and these are crimes that affect the privacy, safety and security of Americans. The Justice Department is taking many steps to respond to the daunting challenges posed by computer crime. In response to this escalating problem, law-enforcement agencies have devoted significant resources to developing teams of investigators and forensic experts who have the specialized skills needed for cyber crime investigations.

The FBI and Secret Service, which are represented here today, have particularly important investigative responsibilities with respect to Internet and computer-related crimes, and they have been in the forefront of this effort, as has the Department of Defense and NASA. On the prosecution side, I am pleased that the Criminal Division has played a particular important role in combating cyber crime.

The centerpiece of our effort is the Criminal Division's Computer Crime and Intellectual Property Section. The attorneys in this section focus exclusively on issues relating to computer and intellectual property crime, allowing them to serve as a nationally-recog-

nized source of advice and expertise on cyber crime law. In addition to responding daily for requests for information and advice from the field, CCIPS' attorneys coordinate multidistrict cases, like the denial-of-service attacks last year, and work extensively with international counterparts to improve legal and operational support for multinational cases.

As well in the Criminal Division, other sections have had to develop computer expertise as traditional forms of crime have moved on to the Internet. As you have noted, Mr. Chairman, the Fraud Section has developed special programs to deal with the dramatic growth in Internet fraud, which is affecting all of us in this country, various types of fraudulent online schemes, and our Child Exploitation and Obscenity Section has strongly promoted the department's efforts against one of the most distrubing facets of cyber crime, the exploitation and abuse of children by online sexual predators and through the distribution of child pornography over the Internet.

We recognize, Mr. Chairman, that our success in this area depends on building networks of cooperation. We're working closely with State and local law-enforcement on operations and training. We're working with international law-enforcement because we realize that cyber crime recognizes no international boundaries. We're working with the private sector to promote information-sharing on our vulnerabilities. Our efforts in these regards are, not surprisingly, documented on the Web site, the CCIPS web site, www.cybercrime.gov.

Mr. Chairman, while the department does all it can to combat cyber crime, Congress can lend substantial assistance to our efforts. In particular, I would like to highlight three areas that merit particular attention. First, Congress should examine the substantive computer crime law, the Computer Fraud and Abuse Act. Given recent virus attacks that have caused damages in the billions of dollars, Congress should assure that the act's coverage is comprehensive and that the penalties for these crimes are commensurate with the harms caused.

Second, Congress should examine the procedural laws that govern law-enforcement investigations in the electronic environment. For example, the statute that governs pen registers and trap and trace devices should be clarified to assure that the privacy protections afforded the users of telephones will equally protect e-mail communications. Similarly, antiquated rules which govern the procedure for tracing a communication when it passes out of the jurisdiction of the local court that issued the pen trap order, should be examined and revised.

Under current law, law-enforcement authorities must apply for the identical order in multiple jurisdictions, causing burdens and delays that benefit no one but criminals. Congress should look at the possibility of a single order that would cover these kinds of requests comprehensively.

Third, a perceived or possible conflict between the Cable Act and the record-keeping statutes that govern telephone companies and Internet service providers has created roadblocks for important law-enforcement investigations, now that cable companies are offering telephone and Internet service. Congress should consider clari-

fying these laws to ensure that the rules governing law-enforcement access to the records of a service provider—a service provider's customers—do not depend on whether the service happens to be transmitted over cable lines, telephone lines or some other medium.

Finally, there is the critical issue of resources. The department can work effectively to combat cyber crime only if we have adequate resources to hire, equip and train investigators and prosecutors. We stand ready to assist you in any way we can as you consider these pressing issues.

Mr. Chairman, all of us are deeply concerned about the safety and security——

Mr. SMITH. Mr. Chertoff, this being the second week that you've been head of the Criminal Division, we have given you a little extra time. But we need to conclude if we can.

Mr. CHERTOFF. I appreciate that, Mr. Chairman. I simply want to say we're all concerned about safety and security. We want to balance it with privacy. That concludes my prepared statement. I am, of course, pleased to answer any questions.

[The prepared statement of Mr. Chertoff follows:]

PREPARED STATEMENT OF MICHAEL CHERTOFF

Mr. Chairman and Members of the Subcommittee, thank you for this opportunity to testify about the Department of Justice's efforts to fight cybercrime. The issue before this Subcommittee today is one of singular importance, and I commend the Subcommittee for holding this hearing.

In my testimony today, I would like to outline briefly the nature of the cybercrime problem and the Department's current efforts to combat that problem. As this is only my second week as head of the Criminal Division, I have not yet had the opportunity to undertake a full review of the problem and how we can best confront it. However, it is clear to me that cybercrime is an extremely serious threat, and that its complexity and constant evolution present a tremendous challenge to law enforcement.

THE NATURE AND SEVERITY OF CYBERCRIME

Over the last decade, use of computers and the Internet has grown exponentially. Indeed, for many individuals it is an integral part of their daily lives. With little more than a click of a mouse, people can communicate, transfer information, engage in commerce, and expand their educational opportunities. Unfortunately, criminals exploit these same technologies to commit crimes and harm the safety, security, and privacy of us all. Indeed, as more people go online, more criminals are realizing that online crime can be lucrative, especially given the amount of valuable commercial and personal information now being stored electronically.

So-called "cybercrime" can be divided into two categories. On the one hand, we are seeing the migration of "traditional" crimes from the physical to the online world. These crimes include threats, child pornography, fraud, gambling, extortion, and theft of intellectual property. Simply put, criminals are migrating online because they can reach more victims quickly, can collaborate with other criminals, can disguise their identities, and can use the global nature of the Internet to remain anonymous.

On the other hand, the Internet has spawned an entirely new set of criminal activity that targets computer networks themselves. Included in this category are such crimes as hacking, releasing viruses, and shutting down computers by flooding them with unwanted information (so-called "denial of service" attacks). Our vulnerability to—and the damages caused by—this type of crime are astonishingly high.

For example, in May of last year, the "I Love You" Virus began to infect computers on the Internet. Within a short period of time, it had disrupted the communications of hundreds of thousands of computers, causing losses estimated in the billions of dollars. Just as disturbing, this virus demonstrated a new capability: when it infected a computer, it accessed the user's computer passwords and sent them electronically to a computer in a foreign country. The implications of this virus—and the many viruses that have followed it—are staggering.

In March of this year, the FBI's National Infrastructure Protection Center issued a warning that an organized group of hackers from Russia and Eastern Europe had committed a series of intrusions into more than forty banks and e-commerce companies in the United States. The hackers stole over 1,000,000 credit card numbers from the companies' data bases. They then embarked on extortion of many of the companies, threatening to disclose confidential information or damage the victims' computer systems. Evidence suggests that the hackers then sold many of the credit card numbers to organized crime groups.

This crime—the investigation into which the Treasury Department participated and which has to date resulted in two arrests—has grave implications. Not only did it cause financial losses for the companies, but it harmed the privacy and security of the ordinary citizens whose credit cards numbers and personal data were stolen. Individuals victimized by these sorts of crimes rightfully fear the ramifications of criminals' gaining access to their private financial and personal data. Moreover, this kind of crime strikes at the confidence of consumers, threatening the vital growth of e-commerce.

Network crimes not only affect the security of individuals and businesses, they can also threaten our nation's critical infrastructures. Our power and water supply systems, telecommunications networks, financial sector, and critical government services, such as emergency and national defense services, all rely on computer networks. This reliance on computer networks creates new vulnerabilities.

For example, for a real-world terrorist to blow up a dam, he would need tons of explosives, a delivery system, and a surreptitious means of evading armed security guards. For a cyberterrorist, the same devastating result could be achieved by hacking into the control network and commanding the computer to open the floodgates. This is not a purely hypothetical scenario. Several years ago, a juvenile hacker gained unauthorized access to the computers controlling the operations of the Roosevelt Dam in Arizona.

Although there are as yet no definitive statistics on the scope of the problem, there is no doubt that the number of crimes involving computers and the Internet is rising dramatically. For example, the CERT Coordination Center, which was created to warn about computer attacks and viruses, received over 21,000 network crime incident reports last year. This is more than double the number of reports it received the year before. Similarly, a survey conducted by the FBI and the Computer Security Institute recently revealed substantial increases in computer crime. Over 85 percent of the companies and government agencies surveyed reported computer security breaches within the preceding twelve months, up from 70 percent last year. Moreover, researchers at the University of California at San Diego recently reported a methodology that enabled them to count the numbers of denial of service attacks. Their research revealed that 4,000 attacks occur every week. Responding to these threats is a daunting challenge.

JUSTICE DEPARTMENT RESPONSES TO CYBERCRIME

While there is little question that combating cybercrime is a tremendous challenge, it is one the Justice Department must be prepared to meet. I can assure you that the Department is committed to arresting and prosecuting those individuals who operate in cyberspace to threaten the security and privacy of our citizens, to disrupt and damage commerce, and to compromise the integrity and availability of the Internet itself. I am very encouraged by the extent to which our investigators and prosecutors have been building a good enforcement foundation. One need only look at the many success stories reflected on the website of the Computer Crime and Intellectual Property Section, *www.cybercrime.gov*, to see their efforts in this area.

From my perspective, as I begin my assessment of our cybercrime efforts and the direction they should take in the future, at least three themes or elements seem to emerge as particularly important to success in confronting cybercrime: developing specialized expertise, building teamwork and partnerships, and assuring we have legal authorities which are both effective and appropriate in the unique and ever-evolving setting of computers and the Internet.

DEVELOPING SPECIALIZED EXPERTISE

Combating computer crime requires a team of professionals, including investigators, forensic experts, and prosecutors, all of whom have technical expertise. In addition to traditional investigative skills, cybercrime investigators must be well versed in the intricacies of technology to insure that evidence is not lost or overlooked. Forensic experts must know how to handle electronic evidence to protect its integrity for later use at trial, as well as how to recover and analyze digital evidence from

computers with hard drives that store gigabytes of data. And prosecutors must understand the jargon and complexities of high-technology crimes and be able to translate technical evidence into a form understandable to a judge and jury.

In response to the escalating problem, our law enforcement agencies have devoted significant resources to developing cadres of investigators and forensic experts who have the specialized skills needed for cybercrime investigations. The FBI and Secret Service, which have particularly important investigative responsibilities with respect to Internet and computer-related crimes, have certainly been in the forefront of this effort.

On the prosecution side, I am pleased that the Criminal Division has played a particularly important role, not only as a source of specialized cybercrime expertise, but as a key player in the training of local, state and federal agents and prosecutors in the laws governing cybercrime.

At the center of this effort is the Criminal Division's Computer Crime and Intellectual Property Section ("CCIPS"). This team of attorneys focuses exclusively on issues relating to computer and intellectual property crime, allowing them to serve as the nationally recognized source of advice and expertise on cybercrime law. In addition to responding daily to requests for information and advice from the field, CCIPS coordinates multi-district cases, and works extensively with international counterparts to improve legal and operational support for multi-national cases, such as the nationwide investigation of the distributed denial of service attacks in February 2000 that eventually led to the arrest of an individual in Canada. The Section's important outreach and education mission includes publication of significant reference materials for prosecutors such as Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations and Prosecuting Intellectual Property Crimes and an extensive training program in which, last year alone, CCIPS' twenty-one attorneys gave over 200 presentations to prosecutors, agents, judges, technical experts, and government and industry groups.

A particularly important aspect of developing, and then sharing expertise in the field is our nationwide network of federal prosecutors called Computer and Telecommunications Coordinators (or "CTCs")—at least one from each district—who serve as the district's prosecutorial expert on computer crime cases. The CTC initiative was started by CCIPS in 1995, and has been strongly supported by our U.S. Attorneys. CCIPS trains and supports these coordinators specially, so that they, in turn, can serve as a resource for their offices and the law enforcement authorities and concerned industry in their regions of the country.

In the Criminal Division, specialized expertise in combating cybercrime is not confined to CCIPS. Other sections have developed this expertise as traditional forms of criminality have moved onto the Internet.

For example, the Department has seen dramatic growth in various types of fraudulent online schemes, and the Criminal Division's Fraud Section has played a critical role in the Justice Department's response, including overseeing a Department-wide Internet Fraud Initiative begun in 1999. Its work to date has included (1) advising and supporting federal prosecutors throughout the country, including maintenance of an Internet fraud brief bank; (2) developing specialized training on Internet fraud for courses at the Department's National Advocacy Center; (3) publishing extensive materials on the Department's website, *www.internetfraud.usdoj.gov*, in order to promote public understanding of Internet fraud schemes and how to deal with them; and (4) supporting improvements in federal agencies' investigative and analytical resources, including the Internet Fraud Complaint Center, a joint project of the FBI and the National White Collar Crime Center. The Department has also been involved in the related problem of identity theft, in part by providing national coordination of governmental efforts through the Identity Theft Subcommittee of the Attorney General's Council on White Collar Crime.

Of course, one of the most disturbing facets of cybercrime is the exploitation and abuse of children, whether through distribution of child pornography over the Internet or through the horrific conduct of sexual predators who operate online. The FBI, the U.S. Attorneys' Offices, and the Division's Child Exploitation and Obscenity Section have developed special expertise in investigating and prosecuting these crimes and currently devote significant resources to the online aspects of child pornography and luring cases. Moreover, in this area and others, the Department's Office of Legal Education, in conjunction with various components of the Criminal Division, regularly sponsors classes regarding computer crime and electronic evidence.

BUILDING PARTNERSHIPS

As I noted at the beginning of my statement, the second element which seems particularly important to our efforts against cybercrime is partnership building. Of

course, from years as a prosecutor, I know that teamwork is essential to any successful crime-fighting effort. But it strikes me that in the area of cybercrime the need for effective partnerships, is not only especially important but also requires partnerships well outside the traditional law enforcement community.

Certainly the complexity of cybercrime and the breadth, or potential breadth of its impact, are part of the reason. However, another factor is the diversity of interests at play in the cyberworld, and hence in our efforts to combat cybercrime. These include, among others, law enforcement interests, national security interests, privacy interests, and commerical interests. Without partnership, or at least dialogue, we will allow those interests to conflict and collide in ways destructive of our efforts to combat cybercrime.

I would like to briefly describe some of the efforts already underway in the Department to build partnerships at the national and international levels and to engage consumers, organizations and business in a cooperative effort against Internet and computer related crime.

Because of the borderless and real-time nature of the Internet, and thus of cybercrime, we at the federal level need effective partnerships with our law enforcement colleagues at the federal, state and local levels, as well as overseas. A good example of cooperation of the federal level, "Operation Cyber Loss," is described in detail in the testimony of FBI Deputy Assistant Director Kubic.

Certainly, within the United States, an important part of our partnership with state and local counterparts is supporting them in developing the specialized expertise I have already described as so important to our cybercrime efforts. For example, the Department founded and funds the National Cybercrime Training Partnership, a ground-breaking consortium of federal, state, and local entities dedicated to improving the technical competence of law enforcement agents and prosecutors. In addition, we have worked with the National Association of Attorneys General to create a 50-state list of state and local computer crime specialists, posted on the web, so that agents and prosecutors from one jurisdiction can call upon their colleagues in another jurisdiction for assistance in cybercrime matters. Also, our AUSAs specializing in cybercrime—the CTCs—are working in their jurisdictions to train state and local agents and prosecutors.

The challenges on the international level are greater. When we deal with a transborder cybercrime, we need foreign law enforcement counterparts who not only have the necessary technical expertise, but who are accessible and responsive, and who have the necessary legal authority to cooperate with us and assist us in our investigations and prosecutions. The Criminal Division has played a central role in attempting to build these sorts of partnerships internationally, and I expect it to continue to do so.

For example, within the larger law enforcement frame work of the G-8's Lyon Group, there is a Subgroup on High-tech Crime which, from its inception, has been chaired by a senior attorney from CCIPS. One of its important accomplishments was the development of a "24/7 network" which allows law enforcement contacts in each participating country to reach out—24 hours a day, seven days a week—to counterparts in other countries for rapid assistance in investigating computer crime and preserving electronic evidence. The Subgroup has also to date sponsored many meetings, including three major conferences, that have brought together government and private sector representatives of all the G-8 countries to discuss cybercrime issues.

As part of our efforts to forge an effective framework for international partnership, the Department, and in particular the Criminal Division, has been engaged in the lengthy and still ongoing process of negotiating a cybercrime treaty in the Council of Europe. Since those negotiations have not yet concluded, I believe it would be premature to discuss the treaty in detail. Nonetheless, if a solid text emerges, it would be a significant legal instrument to assist us in combating cybercrime.

One aspect of our work on the treaty I do want to note especially, however, is the extent to which we have sought to engage the private sector, some elements of which had expressed concerns about aspects of the evolving draft and about the process at the Council of Europe, whose proceedings in this context have not been open to the public. The United States delegation pressed hard for the COE to depart from past practice and publish working drafts of the text, which it began to do more than a year ago. Thereafter, representatives of the Justice Department, along with those from the State and Commerce Departments—the agencies that form our delegation—met on numerous occasions with industry and privacy groups to hear their concerns. As a result, our delegation worked hard, and with a large measure of success, to obtain a number of changes to the treaty sought by industry and privacy groups.

Of course, our dialogue with industry on the international front is part of a much broader partnership between law enforcement and industry to combat cybercrime and protect the nation's critical infrastructures.

As the builders and owners of the infrastructure that supports cyberspace, private sector companies have primary responsibility for securing and protecting the Internet. CCIPS, the National Infrastructure Protection Center (NIPC), and the CTC network have engaged in regular outreach to industry to ensure that communications channels are open between government and the private sector and to encourage cooperation on efforts to prevent and combat computer and intellectual property crimes. For example, the NIPC, in conjunction with the private sector, has developed the "InfraGard" initiative to expand direct contacts between government and private sector infrastructure owners and operators, and to share information about computer intrusions, vulnerabilities, and infrastructure threats.

Consumers, as the users of the infrastructure, also play an important role in securing the Internet. In the real world, most people understand their responsibilities regarding property: one should take appropriate steps to lock one's doors, but one should not enter other peoples' homes without permission even if they leave their doors unlocked. The Department has been working with the private sector and consumers to promote the same kind of safety precautions and ethics in the online world. One program we initiated with the Information Technology Association of America is the Cybercitizen Partnership, a national campaign to raise awareness about using computers responsibly and to provide educational resources to empower concerned citizens. The Partnership has developed a website, *www.cybercitizenship.org*, which provides information to parents, teachers, and children about online ethics.

Certainly, one of the partnerships most important to our cybercrime efforts—one I believe we strengthen through hearings such as this—is the partnership between the Executive and Legislative branches. Of course, it is in the context of this partnership that we will focus on the third important element in our fight against cybercrime, and that is assuring that we have appropriate and effective legal tools.

ASSURING AN EFFECTIVE LEGAL FRAMEWORK

Given my very recent arrival as head of the Criminal Division, I am not in a position today to make specific recommendations about legislation. However, we are looking at this area closely, and are aware that members of Congress are doing so as well.

What I would like to do is to describe in general terms certain areas where our career investigators and prosecutors have raised concerns about our current legal framework for investigating and prosecuting cybercrime. For example, the adequacy of the penalties for certain computer crimes has been questioned, particularly in the aftermath of the "Melissa" virus case. In that case, even though the defendant caused tens of millions, if not billions of dollars of damage. the maximum penalty was five years imprisonment. Also, some prosecutors have expressed concern that the particular statutory approach for computing the minimum thresholds of damage in computer hacking cases, may in fact allow some significant criminals to go unpunished.

There have also been questions about whether procedural statutes, some enacted more than a decade ago, have withstood the changes brought about by the advance of technology. The Pen Register and Trap and Trace Statute is a good example. The "pen/trap statute" establishes a set of procedures by which law enforcement authorities can collect the non-content information associated with a communication. For telephones, this means the source or destination of calls placed to or from a particular phone. Congress enacted this statute in 1986 to protect privacy by requiring that the law enforcement authorities apply for a court order, allowing only government attorneys (not agents) to apply for such orders, and creating a criminal offense for any who use pen/trap devices without authority.

With the advances in technology, law enforcement authorities and the courts have applied the pen/trap statute to new communications media, such as e-mail. In this context, pen/trap devices can uncover the source—but not the content—of a particular Internet communication. For example, law enforcement authorities obtained a pen/trap order on an e-mail account that was central to locating and arresting James Kopp, who had evaded arrest for three years after being indicted for killing a doctor in front of his wife and child in their home near Buffalo, New York, in 1998.

Although numerous courts across the country have applied the pen/trap statue to communications on computer networks, no federal district or appellate court has explicitly ruled on its propriety. However, certain litigants have begun to challenge the

application of the pen/trap statute to such electronic communications. The pen/trap statute protects privacy and is an important investigative tool. Its application to the cyberworld is vital.

Also, this legislation was passed in an era when telecommunication networks were configured in such a way that, in most cases, the information sought could be obtained by issuing an order to a single carrier. With deregulation, however, a single communication may now be carried by multiple providers. For example, a telephone call may be carried by a competitive local exchange carrier, which passes it to a switch to a local Bell Operating Company, which passes it to a long distance carrier, which hands it to a local exchange carrier elsewhere in the U.S., which in turn may finally hand it to a cellular carrier. Under the structure of the current statute, where a court may only authorize the installation of a pen register or trap device "within the jurisdiction of the court," identifying the ultimate source may require obtaining information from a host of providers located throughout the country—each requiring a separate order. Indeed, in one case the Justice Department needed four separate orders to trace a hacker's communications. You can imagine the concern of our investigators and prosecutors about complying with this procedure when confronted with an urgent need for information to prevent a serious crime or trace one in progress.

Another procedural statute that Congress should consider examining is the Cable Communications Policy Act (the "Cable Act") (47 U.S.C. § 551). Technological advances—and uncertainty about the Cable Act's application to them—have created roadblocks for important law enforcement investigations.

In 1984, Congress passed the Cable Act to regulate government access to records pertaining to cable television service. Of course, at that time, cable companies did not offer Internet access or telephone service. Today, they do. Yet a totally separate legal regime governs government access to records pertaining to telephones and the Internet. These laws include the wiretap statute (18 U.S.C. § 2510 *et seq.*), the Electronic Communications Privacy Act ("ECPA") (18 U.S.C. § 2701 *et seq.*), and the pen/trap statute (18 U.S.C. § 3121 *et seq.*). Cable companies have expressed concern that they may expose themselves to liability for violating the Cable Act if they comply with subpoenas and court orders for telephone or Internet records. This complication has at times delayed or frustrated time-sensitive investigations. It makes little sense for the rules governing law enforcement access to the records of communications customers to depend on the method by which the customer connects to the Internet.

These are only a few of the legislative issues we are now reviewing. I know there are other areas of concern, for example, with respect to further protections for children and safeguarding personal information from unauthorized and even criminal use. Moreover, part of our agenda will inevitably concern resources. Future budget requests for the Division will make adequate resources for our efforts against cybercrime a priority.

Conclusion

Mr. Chairman, I want to thank you again for this opportunity to testify about our efforts to fight crime on the Internet. Citizens are deeply concerned about their safety and security when using the Internet, and we unfortunately have already encountered many examples of serious crimes against individuals and businesses and serious invasions of their privacy by criminals. Enhancing the ability of law enforcement to fight cybercrime both promotes Internet users' safety and security and enhances their privacy by deterring and punishing criminals. The Department of Justice stands ready to work with the Members of this Subcommittee to achieve these important goals.

Mr. Chairman, that concludes my prepared statement. I would be pleased to answer any questions that you may have at this time.

Mr. SMITH. Thank you, Mr. Chertoff.

Mr. Kubic?

STATEMENT OF THOMAS T. KUBIC, PRINCIPAL DEPUTY ASSISTANT DIRECTOR, CRIMINAL INVESTIGATIVE DIVISION, FEDERAL BUREAU OF INVESTIGATION

Mr. KUBIC. Good afternoon, Mr. Chairman and Members of the Subcommittee. I, too, am pleased to be with you today and to discuss some of the work of the FBI, as well as do what I can to enlighten the Committee on the issue of cyber crime today. Rather

than repeat some things which already have been covered, I would submit for the record my full statement at this time.

Mr. SMITH. Without objection, any witness will have their full statement made a part of the record.

Mr. KUBIC. Thank you. I would like to make just a few points. The first is that, cyber crimes are, in fact, unique. The cyber criminal operating in that environment stands much less of a chance of being apprehended and located than many other criminals that we are constantly faced with. The crime is committed oftentimes without the knowledge of the individual who is being victimized, as is the case when computer time is stolen.

Additionally, during the initial stages of a computer crime investigation, it is often difficult to ascertain the objective of the crime or the motive of the crime. So we don't know, at the start these intrusions, for example, if the effort is to steal intellectual property or if the effort is to launch a virus or, in fact, it is just a mere theft to steal credit cards. These problems are not quite as vexing in the real world. Considering the example of a bank robbery, it is very clear when a man enters the bank with a gun, to steal, that he is there to rob the bank, and he leaves behind an awful lot of physical evidence, which is not always the case in the cyber world of investigations.

What little evidence is left in a cyber crime is very perishable and often is gone before the investigators arrive on the scene. Thus, it is the nature of cyber crime which leads to the need for extra or special expertise on the part of the investigators, as well as continuing training throughout the course of the cycle of the investigator's career.

The second point I would like to make is that cyber crimes are evolving, as Assistant Attorney General Chertoff has pointed out. This is an area where there are new crimes that are being conceived of and committed by cyber criminals on a regular basis. Additionally, the rapidly developing technology leaves us in a situation where law-enforcement does play a good bit of catchup in order to stay current and to develop techniques to save and preserve the evidence it has found.

With regard to the FBI's response, there have been two major initiatives. The first was the National Infrastructure Protection Center, which I believe you may be very familiar with. That mission, of NIPC, established 3 years ago, was to identify intrusions, to get word out as to the nature of those, so that security people in the private sector can understand what the issue is, what the vulnerabilities are, and fix those.

There are, in fact, NIPC-trained agent in all 56 FBI field offices; 16 of those offices have full squads devoted to the investigation of intrusions. During the course of the investigation, if it is determined that it is a white-collar crime case, that is, the motive of the intrusion is to steal money, additional resources are brought into the mix, particularly white-collar crime investigators.

The second is the Internet Fraud Complaint Center, and I think that the Chairman has noted some of the results of that investigation or that effort. Established a little more than a year ago, the Internet Fraud Complaint Center serves as a clearinghouse where, in fact, complaints can be received, analyzed and investigative re-

ports submitted to not only Federal investigators, but also State and local investigators.

There is no question that to effectively combat computer crime or cyber crime, it needs a marriage, a task force approach, with not only prosecutors who are skilled and knowledgeable of the law, but also investigators, State, local and Federal. The FBI is, in fact, committed to the safety and security of the cyber world and those who either shop or conduct business in the cyber world, as well as those who visit just to obtain information.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Kubic follows:]

PREPARED STATEMENT OF THOMAS T. KUBIC

GOOD MORNING MR. CHAIRMAN AND MEMBERS OF THE SUBCOMMITTEE ON CRIME. I AM PLEASED TO APPEAR TODAY ON BEHALF OF THE FEDERAL BUREAU OF INVESTIGATION AND SHARE WITH YOUR SUBCOMMITTEE THE FBI'S EFFORTS TO ADDRESS CYBER CRIME.

LET ME BEGIN BY EMPHASIZING THAT THE FBI PLACES A HIGH PRIORITY ON INVESTIGATING CYBER CRIME MATTERS AND IS COMMITTED TO WORKING WITH THIS SUBCOMMITTEE AND ALL OF CONGRESS TO ENSURE THAT LAW ENFORCEMENT AND THE PRIVATE SECTOR HAVE THE NECESSARY TOOLS AND PROTECTIONS TO COMBAT THESE CRIMES. IT IS ONLY WITH THE EFFECTIVE COORDINATION AND COOPERATION BETWEEN ALL LEVELS OF GOVERNMENT AND PRIVATE SECTOR COMPANIES THAT EFFORTS TO COMBAT CYBER CRIME WILL SUCCEED. THE FBI RECOGNIZES AND APPRECIATES THE INTEREST AND EFFORTS OF PRIVATE SECTOR COMPANIES IN PREVENTING CYBER CRIME AS WELL AS THEIR WILLINGNESS TO WORK WITH LAW ENFORCEMENT TO ADDRESS THE PROBLEM.

I WOULD LIKE TO FIRST PROVIDE AN FBI PERSPECTIVE AS TO THE EXTENT OF THE CYBER CRIME PROBLEM ALONG WITH THE UNIQUE CHALLENGES FACED BY LAW ENFORCEMENT IN ADDRESSING IT, AND THEN GIVE YOU AN OVERVIEW OF WHAT THE FBI IS DOING TO ADDRESS THE PROBLEM INCLUDING DETAILS CONCERNING THE INTERNET FRAUD COMPLAINT CENTER AND A RECENT NATIONWIDE INTERNET FRAUD OPERATION.

THE INTERNET IS CHANGING THE WORLD AS WE KNOW IT, AND PROMISES TO CHANGE HOW WE BUY THINGS, HOW WE COMMUNICATE, WHERE WE GET ENTERTAINMENT, NEWS, AND WEATHER, WHERE WE WORK, AND MUCH, MUCH MORE WHILE BRINGING ENORMOUS BENEFITS TO SOCIETY. THE GROWTH AND UTILIZATION OF THE INTERNET AS A COMMUNICATIONS AND COMMERCE TOOL IS UNSURPASSED IN MODERN HISTORY. CURRENT TRENDS REFLECT THIS REMARKABLE GROWTH:

- INTERNET USERS IN THE U.S. REACHED 65 MILLION IN 1998, OVER 100 MILLION IN 1999, AND ARE EXPECTED TO EXCEED 200 MILLION THIS YEAR.[1]
- BUSINESS-TO-BUSINESS E-COMMERCE TOTALED OVER $100 BILLION IN 1999 (MORE THAN DOUBLING FROM 1998) AND IS EXPECTED TO GROW TO OVER ONE TRILLION DOLLARS BY 2003. WORLDWIDE NET COMMERCE, BOTH BUSINESS-TO-BUSINESS AND BUSINESS-TO-CONSUMER, WILL HIT AN ESTIMATED $6.8 TRILLION IN 2004.[2]

THE VAST MAJORITY OF COMMUNICATION AND COMMERCE CONDUCTED VIA THE INTERNET IS FOR LAWFUL PURPOSES. HOWEVER, THE INTERNET IS INCREASINGLY UTILIZED TO FOSTER FRAUDULENT SCHEMES. JUST AS PRIOR TECHNOLOGICAL ADVANCES HAVE BROUGHT DRAMATIC IMPROVEMENTS FOR SOCIETY, THEY HAVE ALSO CREATED NEW OPPORTUNITIES FOR WRONGDOING. THE UNIQUE CHALLENGES FACING LAW ENFORCEMENT IN ADDRESSING CYBER CRIME REVOLVE AROUND THE NEBULOUS NATURE OF CYBER CRIME. THE INITIAL STAGES OF A CYBER CRIME INVESTIGATION INVOLVE A HIGH DEGREE OF UNCER-

[1] New York Times, November 12, 1999

[2] Source: Forrester Research, Inc., <http://www.Forrester.com>

TAINTY. IT IS OFTEN DIFFICULT TO QUICKLY IDENTIFY AND ASSESS WHAT TYPE OF CRIME, IF ANY, HAS BEEN COMMITTED. FOR EXAMPLE, WHEN THE FBI RECEIVES A COMPLAINT INDICATING THAT A BUSINESS HAS EXPERIENCED SOME TYPE OF INTRUSION INVOLVING ITS COMPUTER NETWORK, THE POSSIBLE CRIMES COMMITTED ARE INDETERMINATE. IT COULD BE A MALICIOUS HACKING INCIDENT AIMED AT DAMAGING OR SABOTAGING THE NETWORK, A POSSIBLE TERRORIST ATTACK, SOME FORM OF ESPIONAGE, A DENIAL OF SERVICE ATTACK, AS WELL AS ANY MYRIAD FORM OR COMBINATION OF TRADITIONAL CRIMES SUCH AS FRAUDS OR EXTORTIONS. CONTRAST THIS WITH A MORE TRADITIONAL CRIME IN THE PHYSICAL WORLD SUCH AS A BANK ROBBERY. WHEN A SUBJECT WALKS INTO A BANK WITH A GUN DEMANDS MONEY, THE TYPE OF CRIME BEING COMMITTED IS ABUNDANTLY CLEAR TO EVERYONE. MOREOVER, IN A BANK ROBBERY, THERE IS TYPICALLY A NUMBER OF PHYSICAL TYPES OF EVIDENTIARY VALUE SUCH AS FINGERPRINTS, SHOE IMPRESSIONS, SURVEILLANCE VIDEO AND/OR PHOTOGRAPHS, MONEY TAKEN, AND SEVERAL WITNESSES. NONE OF THIS IS AVAILABLE IN THE COMMISSION OF AN ON-LINE CRIME. WHAT LITTLE EVIDENCE IS AVAILABLE IN AN ON-LINE CRIME WILL USUALLY NOT EXIST FOR LONG. WITHOUT AN IMMEDIATE RESPONSE BY SKILLED CYBER INVESTIGATORS, IT WILL OFTEN BE FOREVER LOST.

THIS ELUSIVE NATURE OF CYBER CRIME TRANSLATES INTO A CRITICAL NEED FOR HIGH LEVELS OF EXPERTISE IN INVESTIGATING CYBER CRIME MATTERS. IT IS RARELY CLEAR AT THE OUTSET OF AN INVESTIGATION AS TO THE ULTIMATE PURPOSE BEHIND A COMPUTER INTRUSION. HOWEVER, OUR INVESTIGATIONS HAVE DEVELOPED EVIDENCE THAT IN A MAJORITY OF CASES, THE PURPOSE OF INTRUSIONS IS TO FACILITATE ONGOING CRIMINAL ACTIVITY AND SEEK FINANCIAL GAIN.

BY WAY OF EXAMPLE, ON MARCH 1, 2000, A COMPUTER HACKER ALLEGEDLY COMPROMISED MULTIPLE E-COMMERCE WEB SITES IN THE U.S., CANADA, THAILAND, JAPAN AND THE UNITED KINGDOM, AND APPARENTLY STOLE AS MANY AS 28,000 CREDIT CARD NUMBERS WITH LOSSES ESTIMATED TO BE AT LEAST $3.5 MILLION. THOUSANDS OF CREDIT CARD NUMBERS AND EXPIRATION DATES WERE POSTED TO VARIOUS INTERNET WEB SITES. AFTER AN EXTENSIVE INVESTIGATION, ON MARCH 23, 2000, THE FBI ASSISTED THE DYFED POWYS (WALES, UK) POLICE SERVICE IN A SEARCH AT THE RESIDENCE OF THE SUBJECT WHO WAS THEN ARRESTED IN THE UK ALONG WITH A CO-CONSPIRATOR UNDER THE UK'S COMPUTER MISUSE ACT OF 1990.

THIS CASE WAS PREDICATED ON THE INVESTIGATIVE WORK BY THE FBI, THE DYFED POWYS POLICE SERVICE IN THE UNITED KINGDOM, INTERNET SECURITY CONSULTANTS, THE ROYAL CANADIAN MOUNTED POLICE (RCMP), AND THE INTERNATIONAL BANKING AND CREDIT CARD INDUSTRY. THIS CASE ILLUSTRATES THE BENEFITS OF LAW ENFORCEMENT AND PRIVATE INDUSTRY, AROUND THE WORLD, WORKING TOGETHER IN PARTNERSHIP ON COMPUTER CRIME INVESTIGATIONS. LOSS ESTIMATES ARE STILL BEING DETERMINED.

AS WORLDWIDE DEPENDENCE ON TECHNOLOGY INCREASES, HIGH-TECH CRIME IS BECOMING AN INCREASINGLY ATTRACTIVE SOURCE OF REVENUE FOR ORGANIZED CRIME GROUPS, AS WELL AS AN ATTRACTIVE OPTION FOR THEM TO MAKE COMMERCIAL AND FINANCIAL TRANSACTIONS THAT SUPPORT CRIMINAL ACTIVITY. CRIMINAL ACTIVITY IN THE CYBER WORLD PRESENTS A DAUNTING CHALLENGE AT ALL LEVELS OF LAW ENFORCEMENT. IN THE PAST, A NATION'S BORDER ACTED AS A BARRIER TO THE DEVELOPMENT OF MANY CRIMINAL ENTERPRISES, ORGANIZATIONS AND CONSPIRACIES. OVER THE PAST FIVE YEARS, THE ADVENT OF THE INTERNET AS A BUSINESS AND COMMUNICATION TOOL HAS ERASED THESE BORDERS. CYBER CRIMINALS AND ORGANIZATIONS POSE SIGNIFICANT THREATS TO GLOBAL COMMERCE AND SOCIETY.

THE USE OF THE INTERNET FOR CRIMINAL PURPOSES IS ONE OF THE MOST CRITICAL CHALLENGES FACING THE FBI AND LAW ENFORCEMENT IN GENERAL. UNDERSTANDING AND USING THE INTERNET TO COMBAT INTERNET FRAUD IS ESSENTIAL FOR LAW ENFORCEMENT. THE FRAUD BEING COMMITTED OVER THE INTERNET IS THE SAME TYPE OF WHITE COLLAR FRAUD THE FBI HAS TRADITIONALLY INVESTIGATED BUT POSES ADDITIONAL CONCERNS AND CHALLENGES BECAUSE OF THE NEW ENVIRONMENT IN WHICH IT IS LOCATED. THE ACCESSABILITY OF SUCH AN IMMENSE AUDIENCE COUPLED WITH THE ANONYMITY OF THE SUBJECT,

REQUIRE A DIFFERENT APPROACH. THE INTERNET IS A PERFECT VEHICLE TO LOCATE VICTIMS AND PROVIDE THE ENVIRONMENT WHERE THE VICTIMS DON'T SEE OR SPEAK TO THE FRAUDSTERS. THE INTERNET ENVIRONMENT OFTEN CREATES A FALSE SENSE OF SECURITY AMONG USERS LEADING THEM TO CHECK OUT OPPORTUNITIES FOUND ON THE INTERNET LESS THOROUGHLY THAN THEY MIGHT OTHERWISE. ANYONE IN THE PRIVACY OF THEIR OWN HOME CAN CREATE A VERY PERSUASIVE VEHICLE FOR FRAUD OVER THE INTERNET. THE EXPENSES ASSOCIATED WITH THE OPERATION OF A "HOME PAGE" AND THE USE OF ELECTRONIC MAIL (E-MAIL) ARE MINIMAL. CON ARTISTS DO NOT REQUIRE THE CAPITAL TO SEND OUT MAILERS, HIRE PEOPLE TO RESPOND TO THE MAILERS, FINANCE AND OPERATE TOLL FREE NUMBERS. THIS TECHNOLOGY HAS EVOLVED EXPONENTIALLY OVER THE PAST FEW YEARS AND WILL CONTINUE TO EVOLVE AT A TREMENDOUS RATE.

INTERNET FRAUD DOES NOT HAVE TRADITIONAL BOUNDARIES AS SEEN IN THE TRADITIONAL SCHEMES. NO ONE KNOWS THE FULL EXTENT OF THE FRAUD BEING COMMITTED ON THE INTERNET. NOT ALL VICTIMS REPORT FRAUD, AND THOSE WHO DO, DO NOT REPORT IT TO ONE CENTRAL REPOSITORY. FOR TRADITIONAL FRAUD SCHEMES THE FBI HAS SYSTEMS IN PLACE TO IDENTIFY AND TRACK FRAUD THROUGHOUT THE COUNTRY. FOR EXAMPLE, A CON MAN OPENS UP SHOP IN CHICAGO, FINDS A LOCATION, OBTAINS PHONES, HIRES PERSONNEL, AND BEGINS TO DEFRAUD PEOPLE. WHEN VICTIMS DON'T RECEIVE WHAT THEY WERE PROMISED AND REALIZE THAT THEY HAVE BEEN DEFRAUDED, THEY WILL CONTACT THEIR LOCAL FIELD OFFICE OF THE FBI, AND PROVIDE THE COMPLAINT INFORMATION, WHICH WILL BE FORWARDED TO THE CHICAGO OFFICE (WHERE THE FRAUD IS OCCURRING). THE FBI IN CHICAGO RECEIVES A NUMBER OF THESE COMPLAINTS AND INITIATES AN INVESTIGATION. FRAUD OVER THE INTERNET DOES NOT NEED A PHYSICAL LOCATION, NOR PERSONNEL, NOR TELEPHONES. INTERNET FRAUD IS DISJOINTED, AND SPREAD THROUGHOUT THE COUNTRY AND OTHER COUNTRIES. THE TRADITIONAL METHODS OF DETECTING, REPORTING, AND INVESTIGATING FRAUD FAIL IN THIS VIRTUAL ENVIRONMENT. VICTIMS OF FRAUD HAVE BEEN UNSURE OF HOW OR WHERE TO REPORT WHAT THEY SEE OR WHAT THEY HAVE EXPERIENCED ON THE INTERNET. LAW ENFORCEMENT AGENCIES HAVE RECEIVED COMPLAINTS IN A PIECEMEAL FASHION, MOST NOT REACHING A LEVEL TO ADVANCE THE COMPLAINT TO AN INVESTIGATION. ANOTHER PROBLEM IS VENUE. WITHOUT SOME TECHNICAL INVESTIGATORY STEPS IT IS DIFFICULT TO IDENTIFY THE LOCATION OF A WEBSITE OR THE ORIGIN OF AN E-MAIL.

THE INTERNET PROVIDES CRIMINALS WITH A TREMENDOUS WAY TO LOCATE NUMEROUS VICTIMS AT MINIMAL COSTS. THE VICTIMS OF INTERNET FRAUD NEVER SEE OR SPEAK TO THE SUBJECTS, AND OFTEN DON'T KNOW WHERE THE SUBJECTS ARE ACTUALLY LOCATED. CRIMES COMMITTED USING COMPUTERS AS A COMMUNICATION OR STORAGE DEVICE HAVE DIFFERENT PERSONNEL AND RESOURCE IMPLICATIONS THAN SIMILAR OFFENSES COMMITTED WITHOUT THESE TOOLS. ELECTRONIC DATA IS PERISHABLE—EASILY DELETED, MANIPULATED AND MODIFIED WITH LITTLE EFFORT. THE VERY NATURE OF THE INTERNET AND THE RAPID PACE OF TECHNOLOGICAL CHANGE IN OUR SOCIETY RESULT IN OTHERWISE TRADITIONAL FRAUD SCHEMES BECOMING MAGNIFIED WHEN THESE TOOLS ARE UTILIZED AS PART OF THE SCHEME. THE INTERNET PRESENTS NEW AND SIGNIFICANT INVESTIGATORY CHALLENGES FOR LAW ENFORCEMENT AT ALL LEVELS. THESE CHALLENGES INCLUDE: THE NEED TO TRACK DOWN SOPHISTICATED USERS WHO COMMIT UNLAWFUL ACTS ON THE INTERNET WHILE HIDING THEIR IDENTITIES; THE NEED FOR CLOSE COORDINATION AMONG LAW ENFORCEMENT AGENCIES; AND THE NEED FOR TRAINED AND WELL-EQUIPPED PERSONNEL TO GATHER EVIDENCE, INVESTIGATE, AND PROSECUTE THESE CASES. VICTIMS ARE OFTEN SCATTERED AROUND THE COUNTRY IN DIFFERENT JURISDICTIONS OR COUNTRIES THAN THE SUBJECT(S). SUBJECTS LOCATED IN OTHER COUNTRIES ARE INCREASINGLY TARGETING VICTIMS IN THE U.S. UTILIZING THE INTERNET. EVIDENCE CAN BE STORED REMOTELY IN LOCATIONS NOT IN PHYSICAL PROXIMITY TO EITHER THEIR OWNER OR THE LOCATION OF CRIMINAL ACTIVITY. IN ADDITION, LOSSES SUFFERED BY VICTIMS IN INDIVIDUAL JURISDICTIONS MAY NOT MEET PROSECUTIVE THRESHOLDS EVEN THOUGH TOTAL LOSSES THROUGH THE SAME SCHEME MAY BE SUBSTANTIAL. IN ORDER TO SUB-

POENA RECORDS, UTILIZE ELECTRONIC SURVEILLANCE, EXECUTE SEARCH WARRANTS, SEIZE EVIDENCE AND EXAMINE IT IN FOREIGN COUNTRIES, THE FBI MUST RELY UPON LOCAL AUTHORITIES FOR ASSISTANCE. IN SOME CASES, LOCAL POLICE FORCES DO NOT UNDERSTAND OR CANNOT COPE WITH TECHNOLOGY. IN OTHER CASES, THESE NATIONS SIMPLY DO NOT HAVE ADEQUATE LAWS REGARDING CYBER CRIME AND ARE THEREFORE LIMITED IN THEIR ABILITY TO PROVIDE ASSISTANCE. OUR LEGAL ATTACHE PROGRAM PROVIDES CRITICAL CONTRIBUTIONS IN THESE MATTERS.

CYBER CRIME EXISTS ACROSS FBI PROGRAM BOUNDARIES AND WITHOUT REGARD TO INTERNATIONAL BORDERS. AMONG THE FBI PROGRAM AREAS IMPACTED BY CYBER CRIME ARE: SECURITIES AND COMMODITIES TRANSACTIONS, PRIME BANK SCHEMES, TELEMARKETING SCHEMES, ONLINE BANKING FRAUDS, GOVERNMENT PROGRAM AND PRIVATE HEALTH CARE FRAUD SCHEMES, ONLINE PHARMACY SCHEMES, ONLINE AUCTION FRAUDS, IDENTITY THEFT, INTELLECTUAL PROPERTY THEFT, BUSINESS-TO-BUSINESS FRAUDS, NON-DELIVERY OF SERVICES, SO-CALLED NIGERIAN LETTER SOLICITATIONS, CREDIT CARD FRAUD, E-COMMERCE AND TRADING, E-COMMERCE AND GOVERNMENT PROCUREMENT, ONLINE GAMBLING, ORGANIZED CRIME/DRUGS, TERRORISM, FUGITIVES, PURCHASE AND SALE OF STOLEN/COUNTERFEIT MERCHANDISE, CHILD PORNOGRAPHY, DENIAL OF SERVICE ATTACKS, INTRUSIONS, MONEY LAUNDERING, AND AS A BUSINESS TOOL TO TRANSACT CRIMINAL ACTIVITY.

CRIMINALS COMMONLY USE COMPUTERS TO COMMUNICATE, STORE INFORMATION, AND PERFORM FINANCIAL AND OTHER TRANSACTIONS. INFORMATION WHICH AT ONE TIME WAS MAINTAINED IN PAPER FILES NOW RESIDES IN DIGITAL FORMAT ON HARD DRIVES AND NETWORKS, AND INFORMATION THAT ONCE WAS TRANSMITTED AS ANALOG VOICE OVER TELEPHONE CONNECTIONS IS NOW TRANSMITTED IN DIGITAL FORMAT OVER THE INTERNET. THE RESULT IS THAT THESE DEVICES OFTEN CONTAIN CRITICAL EVIDENCE OF CRIMINAL ACTIVITY NOT ONLY WITH RESPECT TO COMPUTER CRIMES, BUT ALSO WITH RESPECT TO CONVENTIONAL CRIMES WHERE USE OF A COMPUTER IS MERELY INCIDENTAL TO THE CRIME.

IN ADDITION TO THE BASIC INVESTIGATIVE STEPS REQUIRED IN ANY INVESTIGATION, CYBER CRIME INVESTIGATIONS REQUIRE THAT NEW TYPES OF QUESTIONS BE ASKED, NEW CLUES LOOKED FOR, AND NEW RULES BE FOLLOWED CONCERNING THE COLLECTION AND PRESERVATION OF EVIDENCE. IN ORDER TO SUCCESSFULLY CONDUCT THESE INVESTIGATIONS, INVESTIGATORS REQUIRE SIGNIFICANTLY ADVANCED SKILLS. REGARDLESS OF WHETHER THE COMPUTER SYSTEM ITSELF IS THE TARGET OF CRIMINAL ACTIVITY OR THE COMPUTER SYSTEM (OR INTERNET) IS USED IN FURTHERANCE OF A CRIME, THE FACT THAT A COMPUTER IS INVOLVED BRINGS INTO PLAY AND CREATES A NECESSITY AND REQUIREMENT FOR A QUALIFIED PERSON TO COMPETENTLY HANDLE THE COMPUTER-RELATED AND INTERNET ISSUES. COMPUTER ANALYSIS AND RESPONSE TEAM (CART) RESOURCES ARE HEAVILY RELIED UPON BY FIELD OFFICES TO RESPOND TO THE WIDE VARIETY OF COMPUTER FACILITATED CRIMES. THE FBI HAS SUPPORTED LOCAL REGIONAL COMPUTER FORENSIC LABS (RCFL) INITIATIVES IN SAN DIEGO AND DALLAS. THESE COOPERATIVE VENTURES BETWEEN THE FBI, DEA AND OTHER FEDERAL AGENCIES, AND STATE AND LOCAL LAW ENFORCEMENT PROVIDE COMPUTER FORENSIC SUPPORT TO ALL LAW ENFORCEMENT AGENCIES WITHIN THEIR RESPECTIVE TERRITORIES. THE DEVELOPMENT OF SUCH REGIONAL LABS IS, IN OUR VIEW, VERY IMPORTANT, BOTH IN ORDER TO LEVERAGE LAW ENFORCEMENT RESOURCES AND TO ENSURE THE DEVELOPMENT AND IMPLEMENTATION OF SOUND NATIONAL STANDARDS FOR COMPUTER FORENSICS.

TO THIS POINT, WE HAVE DISCUSSED IN GENERAL THE POTENTIAL THREAT POSED BY CYBER CRIME, WHY IT HAS BECOME AND WILL CONTINUE TO BE ONE OF THE MOST SIGNIFICANT CRIME PROBLEMS , AND BRIEFLY DESCRIBED SOME OF THE MYRIAD FACETS OF CYBER CRIME. I WOULD LIKE TO NOW FOCUS THE DISCUSSION ON WHAT THE FBI IS DOING TO ADDRESS THE AREA OF CYBER CRIME.

INTERNET FRAUD COMPLAINT CENTER (IFCC)

THE DEVELOPMENT OF A PROACTIVE STRATEGY TO INVESTIGATE INTERNET FRAUD THROUGH THE ESTABLISHMENT OF AN INTERNET FRAUD COMPLAINT CENTER (IFCC) AS A CENTRAL REPOSITORY FOR CRIMINAL COMPLAINTS WAS ESSENTIAL. THE IFCC IS A JOINT OPERATION WITH THE FBI AND THE NATIONAL WHITE COLLAR CRIME CENTER (NW3C). THE NW3C IS A NON-PROFIT ORGANIZATION WHICH IS PARTIALLY FUNDED BY THE DEPARTMENT OF JUSTICE. THE MISSION OF NW3C IS TO PROVIDE A NATIONWIDE SUPPORT SYSTEM FOR THE PREVENTION, INVESTIGATION AND PROSECUTION OF ECONOMIC CRIMES. A LITTLE OVER A YEAR AGO, ON MAY 8, 2000, THE IFCC OPENED ITS DOORS TO COMBAT THE GROWING PROBLEM OF CRIMINAL FRAUD OVER THE INTERNET. THE IFCC WAS NECESSARY TO ADEQUATELY IDENTIFY, TRACK, AND PROSECUTE NEW FRAUDULENT SCHEMES ON THE INTERNET ON A NATIONAL AND INTERNATIONAL LEVEL. IT SERVES AS A CLEARINGHOUSE FOR THE RECEIPT, ANALYSIS, AND DISSEMINATION OF CRIMINAL COMPLAINTS CONCERNING FRAUDS PERPETRATED OVER THE INTERNET. IFCC PERSONNEL COLLECT, ANALYZE, EVALUATE, AND DISSEMINATE INTERNET FRAUD COMPLAINTS TO THE APPROPRIATE LAW ENFORCEMENT AGENCY. THE IFCC PROVIDES A MECHANISM BY WHICH THE MOST EGREGIOUS SCHEMES ARE IDENTIFIED AND ADDRESSED THROUGH A CRIMINAL INVESTIGATIVE EFFORT.

THE IFCC PROVIDES A CENTRAL ANALYTICAL REPOSITORY FOR CRIMINAL COMPLAINTS REGARDING INTERNET FRAUD, AND IT ACTS AS A RESOURCE FOR ENFORCEMENT AGENCIES AT ALL LEVELS OF GOVERNMENT TO INCLUDE REGULATORY AGENCIES. IT PROVIDES ANALYTICAL SUPPORT, AND AIDS IN DEVELOPING AND PROVIDING TRAINING MODULES TO ADDRESS INTERNET FRAUD. THE FBI AND THE NATIONAL WHITE COLLAR CRIME CENTER (NW3C) COSPONSOR THE IFCC. THIS PARTNERSHIP IS MUTUALLY BENEFICIAL FOR BOTH ENTITIES IN THAT IT ALLOWS BOTH AGENCIES TO SHARE STAFFING RESPONSIBILITIES AND, BY FORWARDING COMPLAINTS TO FBI FIELD DIVISIONS, UTILIZE THE FBI'S INVESTIGATIVE RESOURCES TO ADDRESS THIS NEW TECHNO CRIME.

THE IFCC IDENTIFIES CURRENT CRIME PROBLEMS, AND DEVELOPS INVESTIGATIVE TECHNIQUES TO ADDRESS NEWLY IDENTIFIED CRIME TRENDS. THE INFORMATION OBTAINED FROM THE DATA COLLECTED IS PROVIDING THE FOUNDATION FOR THE DEVELOPMENT OF A NATIONAL STRATEGIC PLAN TO ADDRESS INTERNET FRAUD.

IFCC'S MISSION IS TO DEVELOP A NATIONAL STRATEGIC PLAN TO ADDRESS FRAUD OVER THE INTERNET, AND TO PROVIDE SUPPORT TO LAW ENFORCEMENT AND REGULATORY AGENCIES AT ALL LEVELS OF GOVERNMENT FOR FRAUD THAT OCCURS OVER THE INTERNET.

IFCC'S PURPOSE IS THE FOLLOWING:

- TO DEVELOP A NATIONAL STRATEGY TO ADDRESS INTERNET FRAUD;
- TO DEVELOP CRIMINAL INTERNET FRAUD CASES AND REFER FOR CRIMINAL PROSECUTIONS COMPANIES AND INDIVIDUALS RESPONSIBLE;
- TO REDUCE THE AMOUNT OF ECONOMIC LOSS BY INTERNET FRAUD THROUGHOUT THE UNITED STATES;
- TO PROVIDE AN ANALYTICAL REPOSITORY FOR INTERNET FRAUD COMPLAINTS;
- TO RECEIVE, ANALYZE AND REFER ALL FRAUDULENT ACTIVITY IDENTIFIED ON THE INTERNET;
- TO IDENTIFY CURRENT CRIME TRENDS OVER THE INTERNET;
- TO DEVELOP INVESTIGATIVE TECHNIQUES TO ADDRESS THOSE IDENTIFIED CRIME PROBLEMS;
- TO TRACK FRAUD FACILITATED BY THE INTERNET AND PROVIDE ANALYTICAL SUPPORT OF INTERNET CRIME TRENDS;
- TO ACT AS AN INVESTIGATIVE RESOURCE FOR INTERNET FRAUD;
- TO DEVELOP TRAINING MODULES TO INVESTIGATE INTERNET FRAUD;

- TO DEVELOP INFORMATION PACKETS FROM COMPLAINTS GENERATED AND FORWARD THAT INFORMATION TO THE APPROPRIATE LAW ENFORCEMENT AGENCIES.

PUBLIC AWARENESS OF THE EXISTENCE AND PURPOSE OF THE IFCC IS PARAMOUNT TO THE SUCCESS OF THIS EFFORT. THE IFCC PROVIDES A CONVENIENT AND EASY WAY FOR THE PUBLIC TO ALERT AUTHORITIES OF A SUSPECTED CRIMINAL ACTIVITY OR CIVIL VIOLATION. VICTIMS OF INTERNET CRIME ARE ABLE TO GO DIRECTLY TO THE IFCC WEB SITE *(WWW.IFCCFBI.GOV)* TO SUBMIT THEIR COMPLAINT INFORMATION, RELIEVING CONSIDERABLE FRUSTRATION FOR THE VICTIM IN TRYING TO DECIDE WHICH LAW ENFORCEMENT AGENCY SHOULD RECEIVE THE COMPLAINT. THE FBI WEB PAGE ALSO AIDS IN THIS EFFORT. A DETAILED EXPLANATION OF THE COMPLAINT CENTER, ITS PURPOSE AND CONTACT NUMBERS, IS PROVIDED SO THAT CONSUMERS CAN REPORT INTERNET FRAUD. THE FBI WEB PAGE PROVIDES VICTIMS WITH A HYPERLINK TO THE IFCC WEB PAGE. MANY OTHER WEB SITES WHICH PROVIDE INFORMATION ON FRAUD MATTERS CONTAIN LINKS TO THE IFCC WEB SITE (E.G., THE DEPARTMENT OF JUSTICE SITE, WWW.INTERNETFRAUD.USDOJ.GOV).

THE FBI HAS ALSO ESTABLISHED AN INTERNET FRAUD COUNCIL WORKING GROUP CONSISTING OF FEDERAL AND STATE LAW ENFORCEMENT AGENCIES, INTERNATIONAL LAW ENFORCEMENT AGENCIES, FEDERAL AND STATE ENFORCEMENT AGENCIES, AND REPRESENTATIVES OF THE PRIVATE BUSINESS SECTOR. THE GROUP'S PURPOSE IS TO CREATE A NETWORK TO SHARE INFORMATION, DISCUSS PERTINENT ISSUES, RECOMMEND LEGISLATIVE SOLUTIONS, AND OBTAIN THE MAXIMUM BENEFIT FOR ALL PARTICIPATING MEMBERS.

DURING THE START-UP PHASE OF IFCC, THE ENTIRE STAFF PROCESSED INCOMING COMPLAINTS AND FORWARDED THEM TO LAW ENFORCEMENT AGENCIES. IN ITS FIRST YEAR OF OPERATION, THE IFCC RECEIVED 36,410 COMPLAINTS, OF THOSE COMPLAINTS, 5,907 WERE INVALID, INCOMPLETE OR DUPLICATIVE, RESULTING IN 30,503 VALID CRIMINAL COMPLAINTS. THOSE COMPLAINTS WERE REFERRED TO AN AVERAGE OF TWO TO THREE LAW ENFORCEMENT AGENCIES. THIS REFERRAL PROCESS HAS SPAWNED HUNDREDS OF CRIMINAL INVESTIGATIONS THROUGHOUT THE COUNTRY. THE FBI STAFF AT THE IFCC HAVE BEGUN TO USE THE DATA TO IDENTIFY

MULTIPLE VICTIMS, VARIOUS CRIME TRENDS AND SAME SUBJECT CASES THUS INITIATING THE INVESTIGATIVE PHASE OF THE CENTER'S OPERATIONS. THIS PROCESS WASN'T FULLY FUNCTIONAL UNTIL JANUARY 1, 2001. UTILIZING THIS PROCESS IN WHICH THE IFCC STAFF DRAFT INTERNET INVESTIGATIVE REPORTS AND FORWARDS THOSE REPORTS TO MULTIPLE LAW ENFORCEMENT AGENCIES, THE IFCC HAS INVESTIGATED AND REFERRED 545 INVESTIGATIVE REPORTS ENCOMPASSING OVER 3,000 COMPLAINTS TO 51 0F 56 FBI FIELD DIVISIONS AND 1,507 LOCAL AND STATE LAW ENFORCEMENT AGENCIES. IFCC HAS ALSO REFERRED 41 CASES ENCOMPASSING OVER 200 COMPLAINTS TO INTERNATIONAL LAW ENFORCEMENT AGENCIES. THE IFCC HAS RECEIVED COMPLAINTS OF VICTIMS FROM 89 DIFFERENT COUNTRIES.

AUCTION FRAUD IS BY FAR THE MOST REPORTED INTERNET FRAUD, COMPRISING NEARLY TWO-THIRDS OF ALL COMPLAINTS. PAYMENT FOR MERCHANDISE THAT WAS NEVER DELIVERED ACCOUNTS FOR 22% OF COMPLAINTS, AND CREDIT AND DEBIT CARD FRAUD MAKEUP ALMOST 5% OF COMPLAINTS. ANOTHER 5% OF COMPLAINTS STEM FROM VARIOUS TYPES OF INVESTMENT FRAUDS AND CONFIDENCE FRAUD SCHEMES SUCH AS HOME IMPROVEMENT SCAMS AND MULTI-LEVEL MARKETING SCHEMES. IT HAS BEEN THE EXPERIENCE OF THE FBI THAT FURTHER INVESTIGATION INTO THESE COMPLAINTS OFTEN REVEALS A VARIETY OF FRAUDS BEING PERPETRATED BY SUBJECTS. SUBJECTS ENGAGED IN ONE TYPE OF FRAUD SCHEME SUCH AS ON-LINE AUCTION FRAUD ARE FREQUENTLY INVOLVED IN OTHER TYPES OF FRAUD SCHEMES SUCH AS BANK FRAUD, INVESTMENT FRAUDS AND/OR PONZI/PYRAMID SCHEMES.

BUSINESSES THAT CONDUCT A SIGNIFICANT AMOUNT OF COMMERCE OVER THE INTERNET ARE EXPOSED TO LOSSES IN THE MILLIONS OF DOLLARS DUE TO VARIOUS FRAUD SCHEMES. WITH ASSISTANCE FROM THE PRIVATE SECTOR, THE IFCC IS DEVELOPING A BUSINESS-FRIENDLY SYSTEM FOR RAPID DATA TRANSFER OF MULTIPLE COMPLAINTS IN AN EF-

FORT TO BETTER SERVE THESE CRIME VICTIM-COMPANIES' NEEDS. THIS PROCESS WILL PERMIT THE INTERNET COMPANIES THAT ARE EXPERIENCING THESE LOSSES TO FILE BULK COMPLAINTS AND THOSE COMPLAINTS WILL THEN BE DISTRIBUTED BY IFCC TO THE APPROPRIATE LAW ENFORCEMENT AGENCIES.

IN EFFECT, THE IFCC OPERATES AS PART OF A CYBER COMMUNITY WATCH IN WHICH THE SELF POLICING EFFORTS OF HONEST AND VIGILANT INTERNET USERS AND INTERNET SERVICE PROVIDERS RESULT IN POTENTIAL FRAUDULENT ACTIVITY OVER THE INTERNET BEING BROUGHT TO THE ATTENTION OF LAW ENFORCEMENT THROUGH THE IFCC. THE IFCC DOES MUCH MORE THAN JUST COLLECT COMPLAINT INFORMATION. IT ENSURES THAT THE INFORMATION, ALONG WITH ADDITIONAL INVESTIGATIVE INFORMATION DEVELOPED BY IFCC PERSONNEL, IS DISSEMINATED TO THE APPROPRIATE AGENCIES, AND THAT IDENTIFIED FRAUD SCHEMES CAN BE PREVENTED OR MITIGATED. WHILE OTHER AGENCIES HAVE FRAUD DATABASES THAT COMPLEMENT THAT OF THE IFCC, ONLY THE IFCC PROACTIVELY PROVIDES SUCH INFORMATION TO APPROPRIATE LAW ENFORCEMENT AGENCIES. THE IFCC PROCESSES ALL COMPLAINTS IT RECEIVES REGARDLESS OF THE ALLEGED DOLLAR LOSS. MANY OF THE COMPLAINTS RECEIVED DO NOT ALLEGE LOSSES WHICH MEET MINIMUM DOLLAR THRESHOLDS FOR FEDERAL PROSECUTION, BUT THEY CAN OFTEN BE SUCCESSFULLY WORKED BY LOCAL LAW ENFORCEMENT AGENCIES. AT A MINIMUM, THEY FORM PART OF A DATABASE WHICH ENABLES IFCC TO POTENTIALLY CONNECT THEM WITH A WIDESPREAD FRAUD SCHEME AND/OR ORGANIZED CRIMINAL GROUP. IN THIS LIGHT, ALL COMPLAINTS ALLEGING FRAUD OVER THE INTERNET ARE IMPORTANT. NO VICTIM SHOULD FEEL LIKE ANY LOSS THEY SUFFERED IS TOO INSIGNIFICANT TO REPORT. IT IS ONLY BY VICTIMS AND BUSINESSES REPORTING POTENTIALLY FRAUDULENT ACTIVITY THAT LAW ENFORCEMENT BECOMES AWARE OF IT AND CAN TAKE ACTION. THIS POINT IS MADE CLEAR BY ACTION TAKEN RECENTLY BY THE FBI AND OTHER LAW ENFORCEMENT AGENCIES IN OPERATION CYBER LOSS.

OPERATION CYBER LOSS

THE SUCCESS OF THE IFCC WAS DEMONSTRATED THROUGH IFCC'S KEY ROLE IN OPERATION CYBER LOSS. THE FBI AND THE DEPARTMENT OF JUSTICE ANNOUNCED ON MAY 23, 2001 A NATIONWIDE INVESTIGATION INTO INTERNET FRAUD, CODE NAMED "OPERATION CYBER LOSS," INITIATED BY THE FBI'S INTERNET FRAUD COMPLAINT CENTER (IFCC) AND COORDINATED BY FBI OFFICES, U.S. POSTAL INSPECTION SERVICE (USPIS), INTERNAL REVENUE SERVICE—CRIMINAL INVESTIGATIVE DIVISION, U.S. CUSTOMS SERVICE, UNITED STATES SECRET SERVICE, AND NUMEROUS STATE AND LOCAL LAW ENFORCEMENT ENTITIES. THE INTERNET FRAUD SCHEMES EXPOSED AS PART OF THIS INVESTIGATION REPRESENT OVER 56,000 VICTIMS NATIONWIDE WHO SUFFERED CUMULATIVE LOSSES IN EXCESS OF $117 MILLION. AMONG THE INTERNET FRAUD SCHEMES HIGHLIGHTED BY OPERATION CYBER LOSS WERE THOSE INVOLVING ON-LINE AUCTION FRAUD, SYSTEMIC NON-DELIVERY OF MERCHANDISE PURCHASED OVER THE INTERNET, CREDIT/DEBIT CARD FRAUD, IDENTITY THEFT, VARIOUS INVESTMENT AND SECURITIES FRAUDS, MULTI-LEVEL MARKETING AND PONZI/PYRAMID SCHEMES. APPROXIMATELY 90 SUBJECTS HAVE BEEN CHARGED AS A RESULT OF OPERATION CYBER LOSS FOR WIRE FRAUD, MAIL FRAUD, CONSPIRACY TO COMMIT FRAUD, MONEY LAUNDERING, BANK FRAUD, AND INTELLECTUAL PROPERTY RIGHTS (SOFTWARE PIRACY). TWENTY-SIX DIFFERENT FBI FIELD OFFICES THROUGHOUT THE COUNTRY HAVE BEEN INVOLVED IN THE CYBER LOSS INVESTIGATION. AS IS TRUE OF INTERNET FRAUD IN GENERAL, SUBJECTS AND VICTIMS INVOLVED IN THIS OPERATION WERE SCATTERED THROUGHOUT THE WORLD. ACTION TAKEN IN CONNECTION WITH THIS OPERATION REPRESENTS ONLY A SMALL FRACTION OF CASES REFERRED BY THE IFCC AND ONLY REPRESENT CASES CULMINATING IN SIGNIFICANT PROSECUTIVE ACTION.

THE SCHEMES IDENTIFIED AS PART OF OPERATION CYBER-LOSS VARY WIDELY IN TYPE AND COMPLEXITY. THEY TEND TO BE MULTI-JURISDICTIONAL WITH SUBJECTS AND VICTIMS SCATTERED ACROSS THE UNITED STATES AND THE WORLD. WHILE MANY OF THE SCHEMES INVOLVED AN

ELEMENT OF ON-LINE AUCTION FRAUD, THIS WAS OFTEN ONLY ONE ASPECT OF A SUBJECT'S FRAUDULENT ACTIVITIES. THE CASES REFLECT THE NATURE OF FRAUDSTERS TO MIGRATE FROM ONE FRAUDULENT SCHEME TO ANOTHER, AND IS INDICATIVE OF CRIMINAL BEHAVIOR THAT WOULD ONLY CONTINUE TO EXPAND IF LEFT UNADDRESSED.

THE FBI RECOGNIZES THAT THE IFCC AND INITIATIVES SUCH AS OPERATION CYBER LOSS, WHILE IMPORTANT FIRST STEPS IN ADDRESSING INTERNET FRAUD, REPRESENT MERELY THE TIP OF THE ICEBERG WHEN IT COMES TO THE THREAT POSED BY CYBER CRIME. THEY ARE A PIECE OF A DEVELOPING COMPREHENSIVE FBI STRATEGIC PLAN ADDRESSING ALL ASPECTS OF CYBER CRIME WHICH WILL ALLOW THE FBI AND LAW ENFORCEMENT TO EFFECTIVELY AND EFFICIENTLY MAINTAIN A HIGH LEVEL RESPONSE CAPABILITY AND PROSECUTORIAL SUCCESS IN AREAS WHERE EITHER: (1) A COMPUTER SYSTEM AND/OR THE INTERNET ARE USED IN FURTHERANCE OF A CRIME; OR (2) A COMPUTER SYSTEM IS THE VICTIM OF A CRIME. THE USE OF A COMPUTER SYSTEM OR THE INTERNET IN FURTHERANCE OF CRIME IS NOT LIMITED TO ONE FBI PROGRAM AREA BUT IS INCREASINGLY FOUND IN CRIMINAL INVESTIGATIVE DIVISION AND NATIONAL INFRASTRUCTURE PROTECTION CENTER CASES. IN MANY INSTANCES WHERE A COMPUTER SYSTEM IS SERIOUSLY TARGETED, THE PURPOSE OF THE ATTACK IS TO FACILITATE ONGOING CRIMINAL ACTIVITY.

THE FBI HAS TAKEN A NUMBER OF OTHER STEPS TO ADDRESS CYBER CRIME. THE NATIONAL INFRASTRUCTURE PROTECTION CENTER (NIPC) WAS CREATED IN FEBRUARY, 1998, AND WAS GIVEN A NATIONAL CRITICAL INFRASTRUCTURE PROTECTION MISSION PER PRESIDENTIAL DECISION DIRECTIVE (PDD) 63. THE NIPC MISSION INCLUDES: DETECTING, ASSESSING, WARNING OF AND INVESTIGATING SIGNIFICANT THREATS AND INCIDENTS CONCERNING OUR CRITICAL INFRASTRUCTURES. IT IS AN INTERAGENCY CENTER PHYSICALLY LOCATED WITHIN THE COUNTERTERRORISM DIVISION AT FBI HEADQUARTERS. IN CONJUNCTION WITH THE CENTER, THE FBI CREATED THE NATIONAL INFRASTRUCTURE PROTECTION AND COMPUTER INTRUSION PROGRAM (NIPCIP) AS AN INVESTIGATIVE PROGRAM WITHIN THE COUNTERTERRORISM DIVISION. THE FBI HAS 56 FIELD OFFICES WITH NIPCIP SQUADS WITH 16 REGIONAL NIPCIP SQUADS, WHICH ARE COMPRISED OF SPECIALLY TRAINED INVESTIGATORS AND ANALYSTS. INITIAL INVESTIGATIONS INTO COMPUTER INTRUSION MATTERS HAVE BEEN PRIMARILY CONDUCTED BY NIPCIP SQUADS. DURING THE COURSE OF SUCH INVESTIGATIONS, IT IS INCREASINGLY FOUND THAT THE INTRUSION WAS MERELY THE FIRST STEP IN A MORE TRADITIONAL CRIMINAL SCHEME INVOLVING FRAUD OR OTHER FINANCIAL GAIN. AT THIS POINT IN AN INVESTIGATION, THE CASE WOULD NORMALLY BE TURNED OVER TO THE SUBSTANTIVE SQUAD HANDLING THOSE TYPES OF CRIMINAL SCHEMES. THIS HAS BEEN THE CASE IN NUMEROUS INCIDENTS INVOLVING COMPUTER INTRUSIONS INTO THE DATABASES OF CREDIT CARD COMPANIES, FINANCIAL INSTITUTIONS, ON-LINE BUSINESSES, ETC. TO OBTAIN CREDIT CARD OR OTHER IDENTIFICATION INFORMATION FOR INDIVIDUALS. THIS INFORMATION IS THEN USED IN SCHEMES TO DEFRAUD INDIVIDUALS AND/OR BUSINESSES. DUE TO THE NATURE OF CYBER CRIME AND THE MANNER IN WHICH IT CROSSES TRADITIONAL PROGRAM BOUNDARIES, A NUMBER OF FBI FIELD OFFICES HAVE FORMED "HYBRID" SQUADS WHICH COMBINE NIPCIP, CART, WHITE COLLAR CRIME, VIOLENT CRIME, AND ORGANIZED CRIME/DRUG TRAFFICKING RESOURCES AND INVESTIGATORS ON ONE SQUAD TO ADDRESS CYBER CRIME MATTERS. IN ADDITION, THE FBI CONTINUES TO DEVELOP AND OPERATE CYBER CRIME TASK FORCES CONSISTING OF INVESTIGATORS AND RESOURCES FROM OTHER FEDERAL AGENCIES AS WELL AS STATE AND LOCAL AGENCIES. THE FBI CONSIDERS SUCH TASK FORCES AN EFFICIENT AND EFFECTIVE MEANS TO LEVERAGE RESOURCES AND EXPERTISE IN COORDINATING INVESTIGATIONS INTO CYBER CRIME. THE COMPLEX NATURE OF CYBER CRIME INVESTIGATIONS MAKE COOPERATION AND COORDINATION AMONG LAW ENFORCEMENT AGENCIES VITAL IN THIS AREA. CYBER CRIME TASK FORCES PROVIDE AN INVALUABLE MECHANISM TO COVER INVESTIGATIVE AREAS THAT CROSS JURISDICTIONAL AND PROGRAM LINES. THE FBI PLANS TO AGGRESSIVELY PURSUE DEVELOPMENT OF SUCH TASK FORCES IN ALL FBI FIELD DIVISIONS.

NO LESS IMPORTANT THAN COOPERATION AMONG OTHER LAW ENFORCEMENT AGENCIES IN COMBATING CYBER CRIME IS THE NEED FOR COOPERATION AND COORDINATION BETWEEN LAW ENFORCEMENT AND THE PRIVATE SECTOR. THE FBI CONTINUES TO PLACE A HIGH PRIORITY ON IMPROVING AND DEVELOPING PRIVATE SECTOR OUTREACH PROGRAMS TO FACILITATE REPORTING AND INVESTIGATION OF CYBER CRIME. FOCUS GROUPS HAVE BEEN AND WILL CONTINUE TO BE ESTABLISHED WITH THE PRIVATE SECTOR TO DEVELOP LONG TERM WORKING RELATIONSHIPS WHICH WILL AID IN IDENTIFYING CYBER CRIME PROBLEMS AND THE IMPACT THEY HAVE ON THEIR BUSINESSES AS WELL AS THE FORMATION OF PROACTIVE STRATEGIES TO ADDRESS THE THREATS. THESE RELATIONSHIPS PROMOTE PRIVATE SECTOR REPORTING OF CRIMINAL ACTIVITY, THREAT ASSESSMENT/WARNING TO THE PRIVATE SECTOR AND PRIVATE SECTOR ASSISTANCE TO LAW ENFORCEMENT (SUBJECT MATTER EXPERTISE, TECHNICAL EXPERTISE, ETC.).

FUNDAMENTAL TO THE EFFECTIVENESS OF EFFORTS TO ADDRESS CYBER CRIME ARE IDENTIFICATION AND IMPLEMENTATION OF RECRUITMENT AND TRAINING NEEDS. INTENSIVE TRAINING PROGRAMS ARE NECESSARY TO SUPPORT INVESTIGATIVE EFFORTS AT THE FEDERAL, STATE AND LOCAL LEVELS. CYBER INVESTIGATORS REQUIRE CYBER SKILLS IN THE BASIC PERFORMANCE OF THEIR JOB. THE FBI CURRENTLY PROVIDES SIGNIFICANT BLOCKS OF COMPUTER AND INTERNET TRAINING TO ALL ITS NEW AGENT CLASSES. IN ADDITION, SIMILAR AND MORE ADVANCED TRAINING IS INCREASINGLY PROVIDED TO AGENTS AS PART OF STANDARD ON-GOING TRAINING PROGRAMS.

THE FBI IS COGNIZANT OF ALL THE DIFFICULTIES FACED BY CONGRESS IN CONTEMPLATING ANY PROPOSED LEGISLATION WHICH WOULD AFFECT THE INTERNET. IT REQUIRES A DELICATE BALANCING OF INDIVIDUAL RIGHTS AND POTENTIAL HARM TO SOCIETY; OF FREE COMMERCE AND THREATS TO NATIONAL AND GLOBAL COMMERCE. ON-LINE CHILD PORNOGRAPHY AND THE SEXUAL EXPLOITATION OF CHILDREN PRESENT SUCH ISSUES. WHILE THERE ARE SOME WHO BELIEVE THE FBI'S INNOCENT IMAGES INITIATIVE WHICH UTILIZES UNDERCOVER AGENTS POSING AS CHILDREN ON-LINE TO IDENTIFY AND INVESTIGATE POTENTIAL SEXUAL PREDATORS TO INFRINGE UPON INDIVIDUAL RIGHTS, MOST WOULD AGREE THAT THIS IS OUTWEIGHED BY THE POTENTIAL HARM TO CHILDREN AND SOCIETY IN GENERAL IF THESE SEXUAL PREDATORS ARE NOT STOPPED. THE FBI FULLY SUPPORTS THE DEPARTMENT OF JUSTICE'S VIEW THAT ANY LEGISLATION AFFECTING THE INTERNET SHOULD: 1) TREAT PHYSICAL ACTIVITY AND "CYBER" ACTIVITY IN THE SAME WAY; 2) BE TECHNOLOGY NEUTRAL; AND 3) BE CAREFULLY CRAFTED TO ACCOMPLISH THE LEGISLATION'S OBJECTIVES WITHOUT STIFLING THE GROWTH OF THE INTERNET OR CHILLING ITS USE AS A COMMUNICATIONS MEDIUM.

THE FBI IS COMMITTED TO ENSURING THE SAFETY AND SECURITY OF THOSE WHO USE THE INTERNET WHILE MAINTAINING AN APPRECIATION OF THE INTERNET AS AN IMPORTANT MEDIUM FOR COMMERCE AND COMMUNICATION. FOCUSED LAW ENFORCEMENT EFFORTS WILL PROMOTE GREATER CONSUMER CONFIDENCE AND TRUST IN THE INTERNET AS A SAFE AND SECURE MEDIUM OF COMMERCE AND COMMUNICATION. THE IFCC SERVES AS AN EXAMPLE OF AN INNOVATIVE APPROACH TO AN EMERGING CRIME PROBLEM. IT PROVIDES THE BENEFITS OF COMMUNITY POLICING, FORGING AN EFFECTIVE PARTNERSHIP BETWEEN LAW ENFORCEMENT AT ALL LEVELS, ORDINARY CITIZENS, CONSUMER PROTECTION ORGANIZATIONS SUCH AS THE NW3C, AND THE BUSINESS COMMUNITY. ADDRESSING THE EMERGING AND DYNAMIC THREAT OF CYBER CRIME REQUIRES CONTRIBUTIONS FROM ALL SEGMENTS OF OUR SOCIETY. THE FBI'S IFCC SERVES TO FACILITATE AND COORDINATE THIS COLLABORATIVE EFFORT. THANK YOU.

Mr. SMITH. Thank you, Mr. Kubic.

Mr. Savage?

STATEMENT OF JAMES A. SAVAGE, JR., DEPUTY SPECIAL AGENT IN CHARGE, FINANCIAL CRIMES DIVISION, UNITED STATES SECRET SERVICE

Mr. SAVAGE. Mr. Chairman, Members of the Subcommittee, thank you for the opportunity to address the Subcommittee regarding Federal law-enforcement efforts in combating cyber crime, particularly the efforts of the Secret Service in this regard. I, too, have submitted a comprehensive statement for the record. I would like to summarize; however, before I begin, I would like to acknowledge our partners from the FBI and Department of Justice who assist us in our efforts to combat cyber crime and are critical components in the overall effort.

I will also acknowledge the representative from the Center for Democracy and Technology, which keeps us ever-mindful in respect to keeping the balance between law-enforcement and privacy. The Secret Service fights cyber crime as part of our core mission to protect the integrity of this Nation's financial payment systems. Since our inception in 1865 and an initial mandate to suppress the counterfeiting of currency, modes and methods of payment have evolved and so has our mission. Computers and other chip devices are now the facilitators of criminal activity or the target of such.

In this era of change, one constant that remains is our close working relationship with banking and finance sector. We believe that protection of the banking and financial infrastructure is our core competency area. Mr. Chairman, there's no shortage of information, testimony or anecdotal evidence regarding the nature and variety of cyber-based threats to our banking and financial infrastructures. There is, however, a scarcity of information regarding successful models to combat such crime in today's high-tech environment. That is where the Secret Service can make a significant contribution to today's and future discussions of successful law-enforcement efforts to combat cyber crime.

The Secret Service has developed a highly-effective formula for combating high-tech crime, as demonstrated by our New York Electronic Crimes Task Force. This task force, hosted by the Secret Service, includes 50 different law-enforcement agencies, over 100 different private sector corporations and six different universities. Mr. Chairman, the private sector members of this task force read like a who's-who of the American banking, finance and telecommunications sectors. Companies that have competed tooth and nail with each other in the marketplace come to our task force with a cooperative spirit and a shared goal of preventing computer-based crime and reducing consumer fraud.

The notion of these companies, these competitors and 100 others, sitting down at the same table to share information, knowledge and resources with both each other and with law-enforcement is why we believe we have found a truly unique, innovative and effective formula for combating cyber crime. The task force provides a collaborative crime-fighting environment which reflects our recognition that in today's high-tech electronic crime environment, out-of-the-box problems demand out-of-the-box solutions.

How effective has this task force been? Since 1995, the New York task force has charged over 800 individuals with electronic crimes valued at more than $425 million. It has trained over 10,000 law-

enforcement personnel, prosecutors and private industry representatives in the criminal abuses of technology and how to prevent them. Based on this enormous success of the task force, the Secret Service hopes to replicate the model developed by our New York field office in additional venues around the country in the very near future.

An important component of our investigative response to cyber crime is the Electronic Crimes Special Agent Program. This program is comprised of approximately 175 special agents who have received extensive training in the forensic identification, preservation and retrieval of electronically-stored evidence. We have placed at least one of these highly-trained specialists in every one of our field offices across the country.

Because of the success of the ECSAT program and the boundless nature of electronic crimes, domestic and foreign law-enforcement agencies regularly request training, assistance or seek to exchange information with the Secret Service. As an example, the Secret Service is coordinating with the FBI and NIPC in several areas, to include current investigations involving hackers who have targeted e-commerce sites in the United States. The Secret Service believes there is value in sharing information from our investigations with both those in the private sector and academia, who are devoting substantial resources to protecting their networks and researching new solutions.

Law-enforcement must move from a reactive posture to a proactive or preventative posture by helping its customers to help themselves. The Secret Service learned long ago that our agency needed the full support of others outside our agency to create and maintain a successful and comprehensive security plan during the execution of our protective duties. This predisposition toward discretion and trust naturally permeates our investigative mission where we enjoy quiet successes with our private sector partners.

We have jointly resolved many significant cases with the help of our private sector counterparts, such as network intrusions and compromises of critical information systems. I must point out, however, that such cases are usually not publicized without the express consent of the U.S. Attorney and the victim, because it would breach our confidential relationship and discourage the victims of electronic crimes from reporting such incidents.

Let me relate the Secret Service's mission in fighting cyber crime to the bigger picture of critical infrastructure protection. In this context, our efforts to combat cyber assaults which target information and communication systems which support the financial sector, are part of the larger and more comprehensive critical infrastructure protection scheme. The whole notion of infrastructure protection embodies an assurance and confidence in the delivery of critical functions and services that in today's world are increasingly interdependent and interconnected.

To put this all into perspective, the public's confidence is lost if such delivery systems and services are unreliable or unpredictable, regardless of because the cause of the problem. The Secret Service recognizes that its role in investigating computer-based attacks against the financial sector can be significant in the larger plan for the protection of our Nation's critical infrastructures. When we ar-

rest a criminal who has disrupted a sensitive communications network and are able to restore the normal operation of the host, but it a bank, telecom carrier or medical service provider, we believe we have made a significant contribution toward ensuring the reliability of the critical systems that the public relies upon on a daily basis.

The Secret Service is convinced that building trusted partnerships with the private sector, local law-enforcement and academia is the model for combating electronic crimes in the information age.

If there are any questions, I would be happy to entertain them, and thank you for your time.

[The prepared statement of Mr. Savage follows:]

PREPARED STATEMENT OF JAMES A. SAVAGE, JR.

Mr. Chairman, members of the subcommittee, thank you for the opportunity to address the subcommittee regarding federal law enforcement efforts in combating cyber crime, and particularly the efforts of the Secret Service in this regard.

The Secret Service fights cyber crime as part of our core mission to protect the integrity of this nation's financial payment systems. This role has evolved from our initial mandate to suppress the counterfeiting of currency upon our creation in 1865. Since this time, modes and methods of payment have evolved and so has our mission. Computers and other "chip" devices are now the facilitators of criminal activity or the target of such. The perpetrators involved in the exploitation of such technology range from traditional fraud artists to violent criminals—all of whom recognize new opportunities and anonymous methods to expand and diversify their criminal portfolio.

In this era of change, one constant that remains is our close working relationship with the banking and finance sector. Our history of cooperation with the industry is a result of our unique responsibilities and status as an agency of the Department of the Treasury. We believe that protection of the banking and financial infrastructure is our "core competency" area. As an agency, we seek to manage and apply our investigative resources in the most efficient manner possible for the benefit of our banking and finance customers.

Mr. Chairman, there is no shortage of information, testimony, or anecdotal evidence regarding the nature and variety of cyber-based threats to our banking and financial infrastructures and the need to create effective solutions. There is, however, a scarcity of information regarding successful models to combat such crime in today's high tech environment. That is where the Secret Service can make a significant contribution to today's and future discussions of successful law enforcement efforts to combat cyber crime.

The Secret Service has found a highly-effective formula for combating high tech crime—a formula that has been successfully developed by our New York Electronic Crimes Task Force. While the Secret Service leads this innovative effort, we do not control or dominate the participants and the investigative agenda of the task force. Rather, the task force provides a productive framework and collaborative crime-fighting environment in which the resources of its participants can be combined to effectively and efficiently make a significant impact on electronic crimes. Other law enforcement agencies bring additional criminal enforcement jurisdiction and resources to the task force while representatives from private industry, such as telecommunications providers, for instance, bring a wealth of technical expertise.

Within this New York model, established in 1995, there are 50 different federal, state and local law enforcement agencies represented as well as prosecutors, academic leaders and over 100 different private sector corporations. The wealth of expertise and resources that reside in this task force coupled with unprecedented information sharing yields a highly mobile and responsive machine. In task force investigations, local law enforcement officers hold supervisory positions and representatives from other agencies regularly assume the lead investigator status. These investigations encompass a wide range of computer-based criminal activity, involving e-commerce frauds, intellectual property violations, telecommunications fraud, and a wide variety of computer intrusion crimes.

Since 1995, the task force has charged over 800 individuals with electronic crimes valued at more than $425 million. It has trained over 10,000 law enforcement personnel, prosecutors, and private industry representatives in the criminal abuses of technology and how to prevent them. We view the New York Electronic Crimes Task

Force as the model for the partnership approach that we hope to employ in additional venues around the country in the very near future.

An important component in our investigative response to cyber crime is the Electronic Crimes Special Agent Program (ECSAP). This program is comprised of approximately 175 special agents who have received extensive training in the forensic identification, preservation, and retrieval of electronically stored evidence. Special Agents entering the program receive specialized training in all areas of electronic crimes, with particular emphasis on computer intrusions and forensics. ECSAP agents are computer investigative specialists, qualified to conduct examinations on all types of electronic evidence, including computers, personal data assistants, telecommunications devices, electronic organizers, scanners and other electronic paraphernalia.

The Secret Service ECSAP program relies on the 4-year-old, Treasury-wide Computer Investigative Specialist (CIS) initiative. All four Treasury law enforcement bureaus—the Internal Revenue Service, Bureau of Alcohol, Tobacco and Firearms, U.S. Customs Service and the U.S. Secret Service—participate and receive training and equipment under this program.

All four Treasury bureaus also jointly participate in curriculum development and review, equipment design and distribution of training assets. As a result, financial savings by all Treasury bureaus are realized due to economies of scale. Additionally, agents from different bureaus can work together in the field in an operational capacity due to the compatibility of the equipment and training. In the end, the criminal element suffers and the taxpayer benefits.

Because of the recognized expertise of those in ECSAP, other law enforcement agencies regularly request training from the Secret Service or advice concerning their own computer forensics programs. These requests have come from agencies all across the country, as well as foreign countries such as Italy and Thailand. The Secret Service recognizes the need to promote international cooperation and remains proactive in the dissemination of information to law enforcement agencies, both domestically and internationally, regarding program initiatives and current financial and electronic crimes trends.

Mr. Chairman, we are committed to working closely with our law enforcement counterparts worldwide in response to cyber crime threats to commerce and financial payment systems. This commitment is demonstrated by the Secret Service's effort to expand our overseas presence. We currently have 18 offices in foreign countries and a permanent assignment at Interpol, as well as several overseas initiatives. Recently, new offices have been opened in Frankfurt, Lagos, and Mexico City. The Secret Service is also considering opening new offices in Bucharest and New Dehli. Our expanded foreign presence increases our ability to become involved in foreign investigations that are of significant strategic interest.

In addition to providing law enforcement with the necessary technical training and resources, a great deal more can be accomplished in fighting cyber crime if we are able to harness additional resources that exist outside government in the private sector and academia. The Secret Service believes there is value in sharing information during the course of our investigations with both those in the private sector and academia who are devoting substantial resources to protecting their networks and researching new solutions. On occasion the Secret Service has shared case-specific information derived from our criminal investigations after taking appropriate steps to protect privacy concerns and ensure that there are no conflicts with prosecutorial issues. I would further add that there are many opportunities for the law enforcement community to share information with our private sector counterparts without fear of compromise. The Secret Service recognizes the need for a "paradigm shift" with respect to this type of information sharing between law enforcement and our private sector and academic counterparts.

Finally, law enforcement in general is not sufficiently equipped to train the masses nor can it compete with academic institutions of higher learning in the area of research and development. However, our partnerships with industry and academia have demonstrated that this should be an integral part of the solution.

Partnerships are a very popular term in both government and the private industry these days and everyone agrees that there is great benefit in such an approach. Unfortunately, however, partnerships cannot be legislated, regulated, or stipulated. Nor can partnerships be purchased, traded or incorporated. Partnerships are built between people and organizations who recognize the value in joint collaboration toward a common end. They are fragile entities which need to be established and maintained by all participants and built upon a foundation of trust.

The Secret Service, by virtue of the protective mission for which we are so well known, has always emphasized discretion and trust in executing our protective duties. We learned long ago that our agency needed the full support and confidence

of local law enforcement and certain key elements of the private sector to create and maintain a successful and comprehensive security plan. Furthermore, we are also keenly aware that we need to maintain a trusted relationship with our protectees so that we can work with them and their staffs to maintain the delicate balance between security and personal privacy.

This predisposition towards discretion and trust naturally permeates our investigative mission where we enjoy quiet successes with our private sector partners. We have successfully investigated many significant cases with the help of our private sector partners such as network intrusions and compromises of critical information or operating systems. In such cases, even though we have technical expertise that is second to none, we still rely on our private sector counterparts to collaborate with us in identifying and preserving critical evidence to solve the case and bring the perpetrator to justice. Equally important in such cases is conducting the investigation in a manner that avoids unnecessary disruption or adverse consequences to the victim or business. With the variety of operating platforms and proprietary operating systems in the private sector, we could not accomplish these objectives without the direct support of our private sector counterparts.

In fact, in one recently completed complex investigation involving the compromise of a wireless communications carrier's network, our case agent actually specified in the affidavit of the federal search warrant that representatives of the victim business be allowed to accompany federal agents in the search of the target residence to provide technical assistance. This is unprecedented in the law enforcement arena and underscores the level of trust we enjoy with those we have built relationships with in the private sector. It is also indicative of the complexity of many of these investigations and serves to highlight the fact that we in law enforcement must *work* with private industry to be an effective crime fighting force. In approving this search warrant, the court recognized that in certain cases involving extraordinarily complex systems and networks, such additional technical expertise can be a critical, and sometimes imperative, component of our investigative efforts.

I must point out, however, that such cases are usually not publicized without the express consent of the U.S. Attorney and the corporate victim because it would breach our confidential relationship and discourage the victims of electronic crimes from reporting such incidents.

Four recently-concluded investigations demonstrate the breadth of cases the Secret Service is working, and provide concrete evidence of the continuing success of ECSAP. The cases include the malicious shutdown of a medical service provider's communications system, an intrusion into a telecommunication provider's network, an attack on a private investment company's trading network, and the disruption of a financial institution's complete operating system and communications network.

The first case was initiated on March 5, 2001, when a local Secret Service field office received information that a medical diagnostic service provider had suffered a catastrophic shutdown of its computer network and communications system. The company reported that they were unable to access doctor schedules, diagnostic images, patient information, and essential hospital records, which adversely affected their ability to provide care to patients and assist dependent medical facilities.

Within a matter of hours, a Secret Service ECSAP agent was able to regain control of the network by coordinating with the facility's system administrator to temporarily shutdown and reconfigure the computer system. The ECSAP agent also essentially "hacked" into the compromised system, and modified compromised password files to "lock out" the attacker. This was accomplished while maintaining control of the computer system log files containing evidence of how the intrusion had occurred.

Using this evidence, a federal search warrant was obtained for the residence of a former employee of the hospital, who had recently been terminated from his position as system administrator. Computer equipment was seized pursuant to the warrant, the suspect admitted to his involvement, and federal computer fraud charges are pending.

A case with obvious critical infrastructure implications was initiated on February 20, 2001, when two major wireless telecommunications service providers notified the New York Electronic Crimes Task Force that they had identified two hackers in different remote sites who were attacking their systems. These hackers were manipulating the systems to obtain free long distance service, re-route numbers, add calling features, forward telephone numbers, and install software that would ensure their continued unauthorized access.

The level of access obtained by the hackers was virtually unlimited, and had they chosen to do so, they could have shut down telephone service over a large geographic area, including "911" systems, as well as service to government installations and other critical infrastructure components.

On March 20, 2001, the Secret Service simultaneously executed search warrants in New York City and Phoenix and computer equipment was seized at both locations. One suspect was arrested on federal computer fraud charges, while the other suspect was questioned and released pending a decision by the Department of Justice as to whether or not to pursue federal charges.

The third case occurred from March 9, 2000, through March 14, 2000, when a company located in New York, NY, received several Internet-based "denial of service" attacks on its servers. A "denial of service" attack occurs when a perpetrator launches malicious programs, information, codes, or commands to a target or victim computer which causes a degradation of service or shutdown, thereby denying access by legitimate customers to those computers. In this instance, the company was a prominent provider of electronic trading services on Wall Street.

While the attacks were still occurring, the company's CEO contacted the Secret Service's New York Electronic Crimes Task Force. The CEO identified a former employee as a suspect, based upon the fact that the attacks preyed on vulnerabilities which would only be known to the former employee. These attacks continued through March 13, 2000, when ECSAP agents and task force members identified the attacking computer and arrested the former employee for violating Title 18, USC, Section 1030 (Computer Fraud). In a post-arrest statement, the suspect admitted that he was responsible for the denial of service attacks. As a result of the attacks, the company and its customers lost access to trading systems. Approximately $3.5 million was identified in lost trading fees, commissions, and liability as a result of the customers' inability to conduct any trading.

The last case began just two weeks ago when a financial institution notified local police who in turn notified the local office of the Secret Service, that its entire banking and communications network had been shut down. The institution reported that it was severely crippled, as it had no access to electronic data used in support of its ATMs, banking transactions, employee payroll and all other critical functions. Working with the local police and the bank's technical staff, a former employee emerged as a suspect and electronic evidence was developed that strongly indicated his involvement. The suspect was promptly interviewed by agents and police in which he admitted to disabling the bank's system and "hacking" an unrelated database in his attempts to exact revenge upon the bank CEO. Federal charges are pending.

Let me relate the Secret Service's mission in fighting cyber crime to the bigger picture of critical infrastructure protection. As previously stated, we target cyber crime as it may affect the integrity of our nation's financial payment and banking systems. As we all know, the banking and finance sector comprises a very critical infrastructure sector and one which we have historically protected and will continue to protect. In this context, our efforts to combat cyber assaults which target information and communication systems which support the financial sector are part of the larger and more comprehensive critical infrastructure protection scheme. The whole notion of infrastructure protection embodies an assurance and confidence in the delivery of critical functions and services that in today's world are increasingly interdependent and interconnected. To put this all in perspective, the public's confidence is lost if such delivery systems and services are unreliable or unpredictable regardless of the cause of the problem.

We also recognize that our unique protective responsibilities, including our duties as the lead federal agency for coordinating security at National Special Security Events, demand heightened electronic security awareness and preparation. A well-placed cyber attack against a weak technology or support infrastructure system can render an otherwise sound physical security plan vulnerable and inadequate.

Mr. Chairman, it should also be noted that all deliberate infrastructure attacks, before they rise to such a threshold, are also cyber crimes and are likely to be dealt with initially by law enforcement personnel, both federal and local, in the course of routine business. In fact, I don't believe there is universal agreement as to when a "hack" or network intrusion rises to the threshold of an infrastructure attack and corresponding national security event but we would all probably recognize one when it reached catastrophic proportions.

Given this continuum and interplay between computer-based crimes and national security issues, the Secret Service recognizes that its role in investigating computer-based attacks against the financial sector can be significant in the larger plan for the protection of our nation's critical infrastructures. When we arrest a criminal who has breached and disrupted a sensitive communications network and are able to restore the normal operation of the host—be it a bank, telecommunications carrier, or medical service provider—we believe we have made a significant contribution towards assuring the reliability of the critical systems that the public relies upon on a daily basis.

As a footnote, the Secret Service met recently with representatives of the Financial Services Information Sharing and Analysis Center (FS/ISAC) that was created pursuant to Presidential Decision Directive (PDD) 63. The directive mandated the Department of the Treasury to work with members of the banking and finance sector to enhance the security of the sector's information systems and other infrastructures, a responsibility managed by Treasury's Assistant Secretary of Financial Institutions. The role of the FS/ISAC is to devise a way to share information within the financial services industry relating to cyber threats and vulnerabilities. The Secret Service feels that it can make a significant contribution to the work of the FS/ISAC and is exploring common areas of interest with the FS/ISAC, to include information sharing.

The Secret Service is also continuing to receive requests from local law enforcement agencies and others for assistance, and we welcome those requests. On an alarmingly increasing basis, our local field offices and the Financial Crimes Division of the Secret Service receive desperate pleas from local police departments for physical assistance, training and equipment in the area of computer forensics and electronic crimes so that they can continue to provide a professional level of service and protection for their citizens. In short, the Secret Service has become another option for local law enforcement, the private sector and others to turn to when confronted with network intrusions and other sophisticated electronic crimes.

Over the past 3 years, Secret Service ECSAP agents completed 2,122 examinations on computer and telecommunications equipment. Although the Secret Service did not track the number of exams done for other law enforcement agencies during this period, it is estimated that some 10 to 15 percent of these examinations fell in this category. Many of the examinations were conducted in support of other agencies' investigations such as those involving child pornography or homicide cases simply because the requesting agency did not have the resources to complete the examination itself.

In spite of our limited resources, we do provide physical assistance on a regular basis to other departments, often sending ECSAP agents overnight to the requesting venue to perform computer related analyses or technical consultation. In fact, so critical was the need for even basic training in this regard that the Secret Service joined forces with the International Association of Chiefs of Police and the National Institute for Justice to create the "Best Practices Guide to Searching and Seizing Electronic Evidence" which is designed for the line officer and detective alike. Mr. Chairman, with your permission, I would like to submit a copy of this guide for the record.

We have also worked with this group to produce the interactive, computer-based training program known as "Forward Edge" which takes the next step in training officers to conduct electronic crime investigations. Forward Edge incorporates virtual reality features as it presents three different investigative scenarios to the trainee. It also provides investigative options and technical support to develop the case. Copies of state computer crime laws for each of the fifty states as well as corresponding sample affidavits are also part of the two-CD training program and are immediately accessible for instant implementation.

Thus far we have dispensed over 220,000 "Best Practices Guides" to local and federal law enforcement officers and it is expected that later this summer we will distribute, free of charge, over 20,000 Forward Edge training CDs.

In an additional effort to further enhance information sharing between the law enforcement community and the financial industry, the Secret Service recently created the "E Library" Internet website which serves as a mechanism for all members to post specific information, images and alerts relating to fictitious financial instruments, counterfeit checks, and credit card skimming devices. This website is accessible free of charge to all members of the law enforcement and banking communities and is the only such tool of its kind.

In today's high tech criminal environment, the challenge to federal law enforcement and government is to identify existing repositories of expertise and provide a framework for inclusion and productive collaboration amongst the many government agencies and their respective industry and academic counterparts. The Secret Service is convinced that building trusted partnerships with the private sector and local law enforcement is the model for combating electronic crimes in the Information Age.

Mr. Chairman, that concludes my prepared statement, and I would be happy to answer any questions that you or other members of the subcommittee may have.

Mr. SMITH. Thank you, Mr. Savage.

Mr. Davidson?

STATEMENT OF ALAN B. DAVIDSON, ASSOCIATE DIRECTOR, CENTER FOR DEMOCRACY AND TECHNOLOGY

Mr. DAVIDSON. Thank you. Mr. Chairman and Subcommittee Members, I thank you for this opportunity to testify on the important issue of cyber crime. Thank you for holding this hearing and also for allowing us to participate on a panel with the Government witnesses who are most deeply engaged in dealing with this important issue. The Center for Democracy and Technology is a public interest organization that promotes civil liberties on the Internet.

We have been involved in policy issues surrounding cyber security, privacy and cyber crimes since our formation in 1994. We also coordinate a digital privacy and security working group that includes over 50 companies, public interest groups and associations, who are all thinking hard about how to deal with these issues of privacy and security online.

Mr. Chairman, our Nation is at a point where revolutionary changes in communications and computer technology have created new concerns about public safety, about security and about privacy online. Cyber crime is a serious problem and it demands a real, but limited, response from Government. Our main point today is that as Congress considers cyber crime, it should also strengthen outdated privacy laws. We need to do that in order to restore what is a shifting balance between Government surveillance and personal privacy, in order to build user trust and confidence in what is becoming an economically-vital new medium.

We need to do this in order to afford law-enforcement agencies and online service providers with the clear guidance that they need and that they deserve. In the digital age, the home is exploding. Information that we once kept in our desk drawers is now moving out into electronic form, onto the desktop, and out onto computer networks where it is less secure and less private than it used to be. Our calendars, our checkbooks, our stock portfolios, our diaries, our personal communications, are all making their way out of our possession and onto these networks, where they are afforded far fewer legal protections and fewer of the technical safeguards that used to protect them.

All this contributes to our concern about cyber crime. It also provides new tools for law-enforcement and it shifts the balance that has existed for a long time in terms of our constitutional and legal framework for protecting privacy, both online and offline. It points to the need to rewrite many of the surveillance and privacy laws that were last visited by Congress in 1986, that have been outdated by these technological changes.

I would like to quickly emphasized two major points—two major themes in my testimony. The first is that concerns about cyber crime need not and should not become an excuse for sweeping new authorities or greater Government surveillance capability. The Government has a real, but limited role in protecting security online. On the Internet we have to recognize that users are the most important first line of defense, and it is giving users the tools to protect themselves and the secure systems to operate on that is going to do more to protect security online than anything else that Government can do, and industry is doing a lot in that regard and

I think you will be hearing more about that in your hearing on Thursday.

In that regard, it is not clear that new Government authorities or investigatory powers are needed. Hacking, the distributed denial-of-service attacks, breaking into other people's computers, destroying data, these are all crimes and they should be prosecuted and they are already illegal. Substantial authorities exist for investigating crimes, as well, and I think that on balance we will find that the digital age is actually a net plus for law-enforcement, because it provides access to so much more information than was ever available before.

There is a real risk, however, that concerns about cyber crime will be used as an excuse for implementing much broader kinds of surveillance systems than we have seen before. This point is best underscored by what is happening in Europe right now, where the implementation of a new Council of Europe Convention on Cyber Crime, with new data retention proposals that have recently been proposed or put forward to implement it, are creating huge concerns about personal privacy, cost burdens and changes to the Internet architecture.

Earlier versions of this treaty include very damaging provisions that would have had Internet service providers retaining sensitive information for long periods of time. With the help of the Justice Department, we appreciate that some of the worst provisions of that treaty have been changed, but many parts of it still contain too few limitations on Government action. We will be watching carefully to see how it is implemented.

The second major theme I will cover quickly is just to say that we really do need to strengthen our weak and outdated privacy protections. The last time the Congress revisited the privacy laws was in 1986, before the invention of the World Wide Web, before one out of every two Americans carried cellphones, those laws contained far too few protections or great ambiguities about how law-enforcement gets access to sensitive information like our geographical location.

The extension of pen registers into the Internet introduces new questions about how these rules are going to apply in a world where source and destination information is much more revealing than it ever used to be in the online world, in the telephony world. So I would encourage the Committee to take up a lot of the provisions that it considered last year in H.R. 5018, providing greater protections for all of this information that is out there and is available on the network, and I think that is necessary if we are going to realize the promise of the Internet to protect—promote privacy and individual freedom online.

Thank you.

[The prepared statement of Mr. Davidson follows:]

PREPARED STATEMENT OF ALAN B. DAVIDSON

SUMMARY

Mr. Chairman and Subcommittee Members, thank you for calling this hearing and giving CDT the opportunity to testify about cybercrime. Our nation is at a point where revolutionary changes in communications and computer technology have created new concerns about public safety, security, and privacy online. Cybercrime is a serious problem that demands a real, though limited, response from government.

That response must be crafted recognizing that the digital age also offers tremendous new capabilities for law enforcement, while the rise of personal information online has eroded essential privacy guarantees under law.

As Congress considers cybercrime it should also strengthen outdated privacy laws to restore the shifting balance between government surveillance and personal privacy, to build user trust and confidence in this economically vital new medium, and to afford law enforcement agencies, online service providers, and Internet users the clear guidance they deserve.

This testimony explores three broad themes:

Cybercrime is a serious problem, but must be considered in the context of today's technology, law enforcement capabilities, and eroding personal privacy protections.

- The Internet's unique open and decentralized architecture offers new challenges to traditional approaches to crime. But care must be taken that efforts to address cybercrime do not stifle the innovation or freedom that have been hallmarks of the Internet's success.
- The digital age offers tremendous new tools for law enforcement. The soaring collection of electronic records about online and offline activity have created a wealth of information to investigate and prosecute crimes. On balance, the digital age is likely to be a major net plus for law enforcement capabilities.
- Privacy rules have not kept pace with these changes. Astonishingly, the last significant update to our privacy and surveillance rules came in 1986—before the invention of the World Wide Web, before the Internet became a fixture in schools, homes, and businesses, before more than one in two Americans used mobile phones.

Concerns about cybercrime need not, and should not, become an excuse for sweeping new authorities or greater government surveillance capability.

- The government has a real, but limited, role in promoting security online. The nature of the Internet makes its users the first and most important line of defense against cybercrime, and government alone can do little to guarantee Internet security. Government does have an important role focused on getting its own house in order, training personnel to deal with new technologies, and supporting R&D.
- It is not clear that new government authorities or investigatory powers are needed. Substantial authorities already exist for investigating and prosecuting most cybercrime.
- There is a real risk that cybercrime concerns will become an excuse to implement sweeping new authorities that jeopardize personal privacy. Past efforts to mandate key recovery encryption backdoors, deployment of the "Carnivore" surveillance tool, and expansion of CALEA requirements demonstrate a track record of invasive responses. The point is best underscored in Europe, where implementation of a new Council of Europe Convention on Cybercrime and new data retention proposals are creating huge concerns about personal privacy, cost burdens, and Internet architecture.

Congress should strengthen weak and outdated privacy protections. While improvements to security technology can come from the private sector, only legislation can update the 1980s surveillance and privacy laws in order to provide confidence in the network and resolve gaps and ambiguities in the law. Top priorities should include——

- Providing heightened protections for access to wireless location information, now available for tens of millions of Americans carrying (or driving) mobile phones.
- Increasing the standard for use of pen registers and trap and trace devices, and limiting their use on the Internet since address data for email and Web browsing can be much more revealing than telephone numbers dialed.
- Providing enhanced protection for personal information on networks.

This testimony provides a more detailed list of needed reforms. As a starting point, we would encourage Congress to take up the helpful protections developed and passed by the House Judiciary Committee last September in H.R. 5018 of the last Congress.

It should be noted that nothing in these proposals would deny law enforcement the tools needed to fight crime and defend national security. No law enforcement agency would be prohibited from locating a criminal suspect or monitoring a terrorist's email. All these proposals do is to set clear and strong privacy guidelines for

use of electronic surveillance techniques and require public reporting as the foundation of oversight and accountability.

These are complex issues vital to the future health and growth of the Internet. CDT looks forward to working with the Subcommittee, the Justice Department, and others in the law enforcement community to evaluate cybercrime proposals and to flesh out needed privacy enhancements, in order to restore the trust, security, and privacy consistent with the Internet's promise of promoting economic opportunity and individual freedom.

The Center for Democracy and Technology is a non-profit, public interest organization dedicated to promoting civil liberties and democratic values on the Internet. Our core goals include ensuring that the Constitution[s protections extend to the Internet and other digital media. CDT also coordinates the Digital Privacy and Security Working Group (DPSWG), a forum for more than 50 computer and communications companies, public interest groups, and associations working on information privacy and security.

CONTEXT: LAW ENFORCEMENT CAPABILITIES AND PRIVACY PROTECTIONS IN A DIGITAL AGE

As the Internet becomes increasingly important to consumers and businesses, concerns about criminal activity online and cybercrime are becoming more prevalent. The rapid pace of change has made it harder for Internet users to protect themselves, and creates real challenges for law enforcement.

Concerns about cybercrime are serious. But there are also many reasons to believe the important balance between investigatory powers and individual liberty—enshrined in our legal system and guaranteed by the constitution—has shifted in this digital age, and that greater protections are actually needed for personal privacy. Part of this context is that the digital age offers remarkable and effective investigative tools for law enforcement. At the same time, the amount of personal information available electronically is rising and there is great need for updates in outdated surveillance and privacy law.

The Internet: Rising use, growing concerns, and an eroding balance

The Internet is at once a new communications medium and a new locus for social organization on a global basis. Because of its decentralized, open, and global nature, the Internet holds out unprecedented promise to promote expression, spur economic opportunity, and reinvigorate civic discourse. Individuals and groups can create new communities for discussion and debate, grassroots activism and social organization, artistic expression and consumer protection. The Internet has become a necessity in most workplaces and a fixture in most schools and libraries.

Every day, Americans use the Internet to access and transfer vast amounts of private data. Financial statements, medical records, and information about children] once kept securely in a home or office] now travel through the network. Electronic mail, online publishing and shopping habits, business transactions and Web surfing profiles can reveal detailed blueprints of people[s lives. And as more and more of our lives are conducted online and more and more personal information is transmitted and stored electronically, the result has been a massive increase in the amount of sensitive data available to both potential criminals as well as government investigators.

As social, economic, and personal activities move online, criminal activity taking place or being investigated through the use of the Internet is increasing as well and will likely to continue to increase. One element of concern about cybercrime is the rise of both familiar forms of criminal behavior extended to the instrumentality of the Internet, as well as new harmful acts—such as hacking or identity theft—unique to the digital age. Another concern is the tremendous changes in law enforcement methods that will be needed to adopt to a world where criminal activity is moving off of street corners and into cyberspace. These concerns are exacerbated by new public education problems, as people and business rapidly adopt new online activities without a clear understanding of how to protect themselves and using technologies that may not have adequately accounted for security needs.

A natural reaction in the face of cybercrime concerns is to seek new governmental authorities and powers. A starting point for considering these government actions is the old doctors' adage: First do no harm. There is a real risk that sweeping new mandates or regulations providing incremental improvements in security could undermine many of the open and decentralized features that have been essential to innovation, growth, and freedom online.

More broadly, cybercrime must be addressed in the context of the important protections for individual liberty that stem from the U.S. constitution and are enshrined in our legal system. The Congress and our courts have often denied power-

ful surveillance tools or police powers to the government in order to guarantee basic liberties. In considering cybercrime, it is appropriate to look at both the new capabilities now available to government as well as the eroding state of legal privacy protections.

The Digital Age Presents Tremendous New Tools For Law Enforcement

While the Justice Department frequently complains that digital technologies pose new challenges to law enforcement, it is clear that the digital revolution has also been a boon to government surveillance and collection of information. For example, in testimony last year before a Senate appropriations subcommittee, FBI Director Freeh outlined the Bureau's success in many computer crime cases. Online surveillance and tracking led to the arrest of the Phonemasters who stole calling card numbers; an intruder on NASA computers, who was arrested and convicted in Canada; the thieves who manipulated Citibank's computers and who were arrested with cooperation of Russian authorities; and the creator of the Melissa virus, among others. More recently, alleged hackers who distributed the "I Love You" virus and initiated last year's debilitating distributed denial of service attacks on prominent U.S. web sites have been identified.

In many of these cases, it is the Internet itself that has provided the key instrumentality in investigating and gathering information. Examples include the Justice Department's successful "Innocent Images" campaign to prosecute child pornography, and the recent highly-publicized crackdown on Internet fraud.

Electronic surveillance is going up, not down, in the face of new technologies. Computer files are a rich source of stored evidence: in a single investigation last year, the FBI seized enough computer data to nearly fill the Library of Congress twice. The FBI estimates that over the next decade, given planned improvements in the digital collection and analysis of communications, the number of wiretaps will increase 300 per cent. Online service providers, Internet portals and Web sites are facing a deluge of government subpoenas for records about online activities of their customers. Everywhere we go on the Internet we leave digital fingerprints, which can be tracked by marketers and government agencies alike. The FBI has even requested additional funds to "data mine" these public and private sources of digital information for their intelligence value.

The FBI is also becoming adept at using data collected and stored by the private sector. For example, a recent story in the Wall Street Journal detailed how federal law enforcement agencies have begun purchasing detailed collections of personal data from commercial "look-up" companies. While this raises concerns about agencies skirting the Privacy Act's restrictions on the government's own data collection efforts, it is clear that the FBI is adopting to and using these new and rich data sources.

Privacy Rules Have Not Kept Pace With These Rapid Changes

Another important context for considering cybercrime is that *outdated surveillance and privacy laws have not kept up with changing technology and offer only reduced protections*. Electronic privacy and surveillance are today governed by a complex statutory and constitutional framework that has slowly eroded in the face of technological change.

Remarkably, the 1986 Electronic Communications Privacy Act of 1986 (ECPA), 18 USC 2701 et seq. (setting standards for access to stored electronic communications and transactional records) was the last significant update to the privacy standards of the electronic surveillance laws. Astonishing and unanticipated changes have occurred since then, including——

- the development of the Internet and the World Wide Web, and their widespread use;
- the convergence of voice, data, video, and fax over wire, cable and wireless systems, and the rising deployment of high-bandwidth broadband facilities;
- the increasing use of mobile telephones and devices, including those that access the Internet;
- the proliferation of service providers in a decentralized, competitive communications market; and
- the movement of information out of people's homes or offices and onto networks controlled by third parties.

These changes have left gaps and ambiguities in the surveillance law framework. In some cases, such as the rise of mobile location information or the development of the Web, whole new types of information never available before to law enforcement can now be accessed under a legal framework that never contemplated their

existence. In other cases, such as the use of pen registers for Internet traffic or the standard for accessing location information, the standards and procedures for lawful access are unclear at best.

These gaps create privacy problems, and they also create confusion on the part of law enforcement officers. Greater clarity and enhanced protection is needed both to promote public confidence in law enforcement and to provide deserved guidance about what is and is not acceptable behavior for electronic surveillance and data-gathering.

Most fundamentally, as a result of these changes personal data is moving out of the desk drawer and off of the desktop computer, out onto the Internet and out of personal control. More and more, this means that information is being held and communicated in configurations where it is in the hands of third parties and therefore not afforded the full protections of the Fourth Amendment under current doctrine. In a world where the Internet is increasingly essential for access to commerce, community, and government services, personal privacy should not be the price of living online. Rather, it is necessary to adopt legislative protections that map Fourth Amendment principles onto the new technology.

CONCERNS ABOUT CYBERCRIME NEED NOT, AND SHOULD NOT, BECOME AN EXCUSE FOR SWEEPING NEW GOVERNMENT AUTHORITIES OR GREATER SURVEILLANCE CAPABILITY.

The government has a real, but limited, role in promoting security online.

At the root of many concerns about cybercrime are problems relating to computer security. Hacking, unauthorized access to computers, denial of service attacks, and the theft, alteration or destruction of data are all already federal crimes, and appropriately so. But Internet security is not a problem primarily within the control of the federal government. Particularly, it is not a problem to be solved through the criminal justice system. Internet security is primarily a matter most effectively addressed by the private sector, which has built this amazing, complex and rapidly-changing medium in a short time without government interference.

The government's limited role in cybersecurity stems from the unique technical features of the decentralized, global, user-controlled Internet:

- Unlike traditional broadcast or telecommunications media, where security concerns could be focused on a relatively small number of large companies, today's cybersecurity solutions must apply to literally millions of individuals around the world who create, publish, transmit, route, process, and sell online.
- The Internet's architecture is open, with few (if any) gatekeepers over online activities—a feature essential to the innovation in online services, content, and technologies, and essential to the Internet's promise in promoting free expression worldwide.
- The Internet is global, so the actions of any one national government will only have an incremental effect on behavior and are unlikely to prevent undesirable activity online.

In such an environment, it is the Internet's users who are the first and most important line of defense in the fight against cybercrime. Providing technology to protect users online—such as strong encryption tools and secure software and networks—is likely to be far more effective and scale far better than direct government intervention.

It must be stressed that the source of the security problem is not the architectural openness of the Internet, nor is it inherently a function of the anonymity that openness affords. Indeed, this robust and decentralized architecture is what makes the Internet as resilient as it is. Rather, the problem is that security measures compatible with the open and anonymous nature of the Internet have been given a low priority as the Internet has grown. The explosion of services and business online and the rapid rollout of new software with new features have often come at the expense of good technical security. In that sense, heightened concerns about cybercrime are a helpful wake-up call, not only because they highlight the lack of security but because they also emphasize the bottom line risks.

It is clear that the private sector is stepping up its security efforts, with an effectiveness that the government is not likely to match given the rapid pace of technical change and the decentralized nature of the medium. The tools for warning, diagnosing, preventing and even investigating infrastructure attacks through computer networks are uniquely in the hands of the private sector. In these ways, Internet crime is quite different from other forms of crime.

In this environment, government has an important but limited role focused on getting its own house in order, hiring trained staff, and supporting R&D. First, it

must get its own computer security house in order. The Administratio's National Plan for cyber-security, which focuses on protecting the government[s own systems, has some laudable and long-overdue elements. We are concerned, though, that it relies too heavily on a monitoring system that threatens privacy and other civil liberties ("FIDNet") and gives too little priority to closing the known vulnerabilities and fundamental security flaws in government computer systems. (Target date for fixing "the most significant known vulnerabilities" in critical government computers: May 2003.) To improve government computer security and enforce the computer crime laws, the government needs the resources and Title 5 authority to hire and retain skilled investigators and computer security experts. Law enforcement must undertake the daunting task of training a new generation of public safety officers whose most important weapon is not a gun but a laptop.

The government should do more to support basic research and development in computer security. It is a positive step that the U.S. government has stopped fighting deployment of encryption. We are concerned, though, that a range of new surveillance initiatives ranging from "Carnivore" to CALEA and "wiretapping for the Internet" are being used to build surveillance features without adequate attention to security] and may themselves constitute a security vulnerability. While the potential for the government to help is limited, the risk of government doing harm through design mandates or further intrusions on privacy is very high.

IT IS NOT CLEAR THAT NEW GOVERNMENT AUTHORITIES OR INVESTIGATORY POWERS ARE NEEDED.

Substantial authorities already exist for investigating and prosecuting cybercrime. It appears that most of the "cybercrime" activities conducted online could be prosecuted through existing criminal law. The Computer Fraud and Abuse Act and other statutes broadly make hacking, unauthorized access to computers, and the theft, alteration or destruction of data already federal crimes. Powerful statutes exist to punish distribution of obscenity or child pornography online. Existing criminal statutes covering a range of topics from fraud to abuse of a minor are being applied to or have been adopted to include online behavior.

It is always appropriate to consider whether our laws have been outdated by changes in technology, and several proposals have been under consideration to amend the computer crime statute and the electronic surveillance laws to enhance law enforcement authorities. The Subcommittee, after careful analysis, may find that some modest changes are appropriate. But we urge caution, especially in terms of any changes that would enhance surveillance powers or government access to information. For example, the Justice Department had proposed changes to the computer fraud statutes that would lower the $5000 loss threshold before criminal penalties apply. However, there is reason to believe that prosecutors are unwilling to bring even cases that meet the threshold because of stiff mandatory minimums that apply. Removing the damage threshold would only exacerbate the situation and also could make *de minimus* activity or online pranks serious federal crimes.

Some in government have argued that the Internet requires greater investigatory powers. In particular, they complain about anonymity or lack of traceability on the Internet. This is a red herring. The digital age of web logs, ISP records, credit card transactions, electronic banking, cookies, and clickstreams is creating a wealth of investigatory capability where none existed before. While there is not perfect traceability online, there is probably more traceability online than in the real world. An anonymous vandal can throw a brick through a bank window and run away down any number of streets. An anonymous pickpocket can steal your wallet with credit cards and melt into the crowd. Yet we do not require people to carry identification cards, nor do we install checkpoints on our streets. We do not have perfect traceability in the real world, for good reasons. We do not need perfect identity and traceability online either.

Nonetheless, the Justice Department has sought further expansions in its surveillance authorities. But surely, before enacting any enhancements to government power, we should ensure that current laws adequately protect privacy. For example, the government has proposed extending the pen register statute—designed for capturing digits dialed on a phone—to the Internet. Yet, the current standard for pen registers imposes little effective judicial control, reducing judges to mere rubberstamps. Pen registers as applied to Internet communications are far more revealing than phone numbers, and there is a great deal of ambiguity about how they might be applied online. In this and other cases, we must tighten the standards for government surveillance and access to information, thus restoring a balance between government surveillance and personal privacy and building user trust and confidence in these economically vital new media.

These are complex issues. CDT is prepared to work with the Committee and the Justice Department to evaluate cybercrime proposals, to flesh out needed privacy enhancements, and to convene our DPSWG working group as a forum for building consensus.

THERE IS A REAL RISK THAT CYBERCRIME CONCERNS WILL BECOME AN EXCUSE TO IMPLEMENT SWEEPING NEW AUTHORITIES THAT JEOPARDIZE PERSONAL PRIVACY.

Americans are already deeply concerned about their privacy, especially online. Changes in technology are making ever more information available to government investigators, often with minimal process falling far short of Fourth Amendment standards. There is a real risk that concerns over the very real problems of cybercrime will serve as justification for legislation or other government mandates that will be harmful to civil liberties and the positive aspects of the Internet. Such a course is especially unjustified when there is so much to be done to improve security without changing the architecture or protocols of the Internet or further eroding privacy.

Examples abound already here in the U.S. For much of the last decade, the government has sought to force Internet users to adopt "key recovery" backdoors for their encryption products in the name of fighting crime online—despite the security risks and privacy concerns raised by creating backdoors in security tools. In the name of protecting critical infrastructure, some have promoted "Caller ID for the Internet"—a system of mandatory identification for Internet traffic of dubious practicality that would eliminate much privacy online. While these proposals have been largely rejected "Carnivore"—the FBI's aptly-named Internet surveillance tool—has been deployed despite concerns that it is ripe for abuse and accesses too much information without appropriate legal standards in place. The CALEA statute, passed to preserve government phone tapping capabilities from the specter of digital age communications, has since been expanded to include a wide variety of new services including turning mobile phones into location tracking devices for law enforcement—with little judicial oversight.

It is understandable that many are concerned about new surveillance proposals put forward to fight cybercrime. We have avoided some of the worst of these proposals here in the U.S. Unfortunately, there is evidence that many of the most damaging surveillance proposals are taking root outside of the U.S.

Recent efforts in Europe on cybercrime, and particularly the experience of the recent Council of Europe's proposed Convention on CyberCrime, underscore this point. Early versions of that Convention—developed in part in consultation with U.S. law enforcement officials—contained data retention and other requirements that would have forced ISPs and web services to keep and produce vast quantities of private data at substantial expense and with few privacy protections. Only in response to outcry from industry and public interest advocates were the worst of these provisions modified in recent drafts. But the Convention still contains few privacy protections and lacks an appropriate balance between provisions for law enforcement and preservation of individual rights. We note that the Convention would not require any changes in U.S. law, and we will carefully monitor any efforts to use it as an excuse for changes in the U.S.

A major concern about the COE Convention is how it will be implemented by individual nations. With few clear privacy guidelines built in, it is feared that many will use the Convention as a justification for imposing new design mandates on Internet providers that will threaten many of the Internet's most important characteristics. In recent weeks, a serious proposal has been floated in Europe to require that all Internet traffic be retained for seven years. Besides being impractical and prohibitively expensive, if not virtually impossible, such an effort would be an unprecedented invasion of personal privacy and a severe rollback of initiatives in Europe and elsewhere to *limit* the retention of personal data.

In addition to affecting the human rights of Internet users worldwide, proposals such as these have an impact on U.S. users as well. They risk subjecting consumers and businesses engaging in global Internet communications and commerce to potential surveillance, industrial espionage, or invasions of privacy. And they risk squelching the promise of the Internet as a medium that promotes the free flow of information and the exchange of democratic ideas.

The U.S. has been a force for democratic values, individual liberty, and human rights worldwide. There is a real risk now that cybercrime efforts here and abroad will threaten these very values. It is important that we continue to be an example and resist the temptation to implement cybercrime proposals that would jeopardize the promise of the Internet to promote liberty.

The Need for Enhanced Privacy Protections

Considering the broad sweep of the digital revolution, it is apparent that the major problem now is not that technology is outpacing government's ability to investigate crime, but, to the contrary, that changes in communications and computer technology have outpaced the privacy protections in our laws. Technology is making ever-increasing amounts of information available to government under minimal standards falling far short of Fourth Amendment protections. Gabs in our surveillance laws leave information unprotected, or create ambiguities, ultimately harming public faith in law enforcement and undermining public trust in the online activities that have become such an important part of the digital age.

While improvements to security, technology, or corporate policies to promote privacy can come from the private sector, only legislation can update the legal framework governing electronic surveillance and privacy. Companies can adopt great privacy practices about the disclosure of information, but they have little choice but to produce sensitive data they hold when presented with a lawful order. Consumers and businesses increasingly recognize that only legislation can provide adequate privacy protections for such information and these protections themselves can be a key enabler of trust and security online.

Congress should adopt a comprehensive legislative approach to cybercrime that recognizes the urgent need for additional privacy protections. The Congress could start by taking up the helpful changes to surveillance law developed and passed by the House Judiciary Committee in the last Congress, under H.R. 5018, including:

- Provide heightened protections for access to wireless location information, requiring a judge to find probable cause to believe that a crime has been or is being committed. Today tens of millions of Americans are carrying (or driving) mobile devices that could be used to create a detailed dossier of their movements over time—with little clarity over how that information could be accessed and without an appropriate legal standard for doing so.
- Increase the standard for use of pen registers and trap and trace devices, requiring a judge to at least find that specific and articulable facts reasonably indicate criminal activity and that the information to be collected is relevant to the investigation of such conduct.
- Add electronic communications to the Title III exclusionary rule in 18 USC 2515 and add a similar rule to the section 2703 authority. This would prohibit the use in any court or administrative proceeding of email or other Internet communications intercepted or seized in violation of the privacy standards in the law.

Require a judicial warrant for government seizure of read or unread email stored with a service provider for up to one year. (Currently, the warrant requirement applies for only 180 days, and the government has maintained that it could obtain email with a mere subpoena as soon as it is opened, no matter how recent it is.)

- Require statistical reports for 2703 disclosures, similar to those required by Title III.

Require high level Justice Department approval for applications to intercept electronic communications, as is currently required for interceptions of wire and oral communications.

In addition, other issues—some of broader scope—need to be addressed:

- Define and limit what personal information is disclosed to the government under a pen register or trap and trace order served on Internet service providers. Transactional or addressing data for electronic communications like email and Web browsing can be much more revealing than telephone numbers dialed.
- Define clearly what transactional information can be collected on Internet communications and under what standard, making it clear that Internet queries are content, which cannot be disclosed without consent or a probable cause order.
- Improve the notice requirement under ECPA to ensure that consumers receive notice whenever the government obtains information about their Internet transactions.
- Provide enhanced protection for personal information on networks: probable cause for seizure without prior notice, and a meaningful opportunity to object for subpoena access.

- Require notice and an opportunity to object when civil subpoenas seek personal information about Internet usage.

The bills put before this Committee last year were efforts towards a modest improvement in privacy protections without in any way denying the government any investigative tools. They should serve as a starting point, and we hope that Members will consider reintroducing them in the near future and begin to address the privacy concerns of many Americans and the imbalance that exists in today's electronic surveillance laws.

CONCLUSION

The issue of cybercrime appropriately demands public attention and real, but limited, involvement by government. More broadly, it speaks to the need for modernization of our surveillance laws and greater privacy protections to counteract new threats to privacy online.

Protecting national security and public safety in this digital age is a major challenge and priority for our country. On balance, however, we believe that new sources of data and new tools available will prove to be of great benefit to government surveillance and law enforcement. These new technologies are likely to make law enforcement[s job harder in some ways. There is no doubt that resources will be needed to deal with change as the Internet alters traditional methods of crime fighting and information gathering.

The real cybercrime risk is that concerns about public safety will become a justification for sweeping new surveillance proposals or design mandates that destroy the best features of innovation and freedom on the global, open Internet. It is essential that we offer a measured response to these concerns, and urgently take up the need to reform privacy protections in the electronic surveillance laws.

Mr. SMITH. Thank you, Mr. Davidson.

Mr. Chertoff, let me ask a question that Mr. Coble was going to ask and I would have asked in any case, anyway, and that is what priority is the Administration going to give to the prosecution of intellectual property crimes?

Mr. CHERTOFF. Mr. Chairman, we're going to give it very high priority. I think there's no doubt in this day and age the most valuable kind of property we have this country, in many instances, is intellectual property. It is the source of value for our businesses. It is a source of value for private people and it is something that we have a very serious obligation to protect. One of the reasons we have the section I described in my opening testimony was to concentrate expertise in intellectual property investigations in a group of lawyers who, though experience and education, will become really the cutting edge of these kinds of investigations and prosecutions.

We are aggressively pursuing these crimes. It is a very high priority and we're going to use all the tools we can to pursue it.

Mr. SMITH. Thank you. Let me address my first question to Mr. Chertoff, Mr. Kubic, and Mr. Savage, as well; and it is this: You three individuals have made the point in your testimony that basically our current laws are outdated, much as Mr. Davidson said. Our privacy laws are outdated because we really have not had any legislation since 1986. The same can be said about our high-tech or intellectual property or cyber crime law, I think, particularly in the areas—just to mention three, I would say child pornography, fraud and gambling, perhaps.

In the past, we have had laws that have dealt with these crimes in what you referred to as the physical world, as opposed to the online world. What changes in the laws need to be made to bring our laws up to date so that we can apprehend and convict the cyber criminals? If you will, be specific about what changes you think

need to be made in the laws, because that is really the direction we're heading with these three hearings on this subject. Mr. Chertoff, if you will begin and hen I'll go to the other two individuals.

Mr. CHERTOFF. I will be happy, Mr. Chairman. Obviously, there are two types of laws. There are substantive laws against fraud and child pornography which we can apply, really, equally to the Internet as we do in the physical world. But there also a series of what I would call procedural or process laws, which were written in the last couple of decades at a time when computers and Internet use were really not what they are today.

I will take a concrete example. When you deal with telephony, you have pen registers and traps and traces which allow you to determine, not the content of conversations, but where telephone calls are being placed and where telephone calls are being placed from. In applying that law to the Internet, it has been unclear sometimes to the courts whether the law gives us the authority to use those devices in the world of e-commerce, in the world of the Internet.

By the same token, laws that were written to govern pen registers and trap and trace devices jurisdiction by jurisdiction, court by court, really do not work very well in a world in which data moves internationally with great speed and where we are very happy to go to a judge and get an order under the prevailing legal standard, but it becomes difficult to go to 10 or 15 or 20 judges at one time.

These are the kinds of procedural fixes that we need to bring into law. They don't affect privacy, but they do affect efficiency.

Mr. SMITH. Very good. Thank you.

Mr. Kubic?

Mr. KUBIC. Actually, Mr. Chairman, I cannot add too much to that. I think we have been very effective in working with the Department of Justice in terms of substantively what to charge. The frustration for the investigator comes to the forefront when he or she interacts with the prosecuting attorney and confronts different rules that define what, in fact, can be obtained through the court order. So it is an issue that I think needs some careful study and attention, and I think we can come back with some recommendations for your consideration.

Mr. SMITH. Very good. Thank you.

Mr. Savage?

Mr. SAVAGE. Yes, Mr. Chairman, nothing more to add, other than to make the analogy law-enforcement needs the same tools it has in the physical world, to be able to apply those to the cyber world, with the extra dimension, as previously mentioned, the speed and diffusion of evidence, electronic evidence, is so great that we need greater flexibility in terms of orders or judicial tools that would allow us to get the same information we might have in the physical world, but get it in the cyber world.

Mr. SMITH. Thank you.

Mr. Davidson, I have actually got another question for you that might let you say what you want to say anyway, but in all fairness, if you want to respond, you may.

Mr. DAVIDSON. Well, I just wanted to respond to Mr. Chertoff's comment, because I agree, I think, that the pen register is, for ex-

ample, a great example of an area where we need to revisit the law, but I think to show the complexity of this, there is a feeling that, on the Internet, the notion of extending a statute that was designed to talk about—provide digits dialed on a telephone to law-enforcement on what is a very low legal threshold, based on relevance to an ongoing investigation, reveals much more on the Internet than it did in the context of digits dialed.

Mr. SMITH. Let me get in a quick question, since my time is up, and then, as you said at one point in your testimony, it is not clear that new Government authorities or investigative powers are needed, but then you conceded, I think, the Subcommittee may find that some modest changes are appropriate. Do you want to very quickly tell us what those modest changes are?

Mr. DAVIDSON. Well, I will defer in some ways to Mr. Chertoff's comments about where there are different difficulties in applying the law.

Mr. SMITH. My suspicion was that there was perhaps more agreement than disagreement, and that confirms it, I think, to some extent. Thank you.

The gentlemen from Virginia, Mr. Scott, is recognized for his questions.

Mr. SCOTT. Thank you, Mr. Chairman.

Mr. Savage, you had indicated that some of the banks and others had gotten together to share resources or share ideas. Are there any intellectual property or antitrust implications that we should be addressing and having groups get together like that?

Mr. SAVAGE. Mr. Scott, of course all the participants, especially at the beginning of such efforts, are particular mindful of such concerns. However, after developing personal relationships amongst each other, they realize that, in fact, there are ways to avoid such concerns and still yet be able to share important information and resources. Oftentimes, competitive concerns do not rear their head when you're talking about addressing particular investigative aspects in a generic fashion, about a variety of cases.

Mr. SCOTT. But codes and things like that, software that one bank may have that another one might not have figured out how to do yet, the intellectual property exchanges and the antitrust implications of getting together and agreeing to do things certain ways, are those things that we ought to be looking at to make sure that the antitrust laws and intellectual property laws allow that to happen?

Mr. SAVAGE. Mr. Scott, it is difficult for me to speak for the private sector, but I do know in our conversations with them, they feel like they have been able to overcome a lot of those concerns, but certainly the Government needs to promote avenues and methods for them to more freely exchange information amongst themselves and with us.

Mr. SCOTT. You indicated that you keep secret sine crime reports.

Mr. SAVAGE. I'm sorry?

Mr. SCOTT. You keep secret some reports of cyber crime, so that you would encourage the reporting of the crimes?

Mr. SAVAGE. Absolutely.

Mr. SCOTT. You can't keep it secret and prosecute it at the same time.

Mr. SAVAGE. Mr. Scott, the point I was trying to make is that what is very important to the Secret Service is that when a corporate victim steps forward and raises their hand and says, "We have a problem," or "We have suffered a problem," that we're able to respond in a fashion that addresses their concerns with where they are in the marketplace, their potential public exposure, their operational aspects, their duties to their customers, and to that extent we do not treat that relationship lightly. If there is a success that we do encounter, if it were to be publicized, we would seek their express permission, as well as that of the U.S. Attorney.

It is far more important for the Secret Service to have the success than it is to have others knowing about it.

Mr. SCOTT. Mr. Chertoff, the trap and trace on e-mails, when you get an order allowing this, you have indicated that it is inconvenient to go to different judges. Is your proposal to allow one judge to give an order, regardless of the jurisdiction or are you looking for a blanket order so that once you get the order, you can take it where you want?

Mr. CHERTOFF. I think what we're looking for, Congressman, is the ability to go to a single judge, satisfy the appropriate standard, and have that order apply with nationwide jurisdiction, not be subject only to the particular district in which the judge is sitting.

Mr. SCOTT. Well, if the judge sits and hears that you need a trap and trace, is that just one computer that you're talking about ? If you had several computers, if they were e-mailing within your jurisdiction, would you have to go back to have a trap and trace for each different computer within that jurisdiction?

Mr. CHERTOFF. I don't want to stretch myself beyond my technical competence, so I am going to let Mr. Kubic chime in, but I think it—what we're trying to do, and I use the analogy with the telephone, if you want to get the identity of whoever has generated a particular transmission, typically in the old days with telephony, you could pretty much figure out where the communication was being routed from, what jurisdiction you have to be concerned about.

Nowadays, it is possible to move the communications through a lot of different computers and a lot of different intermediaries, and to avoid a problem, you want to—you know, you technically want to make sure you have covered all of those intermediate stops for the communication. That is what we want to address. I will let Mr. Kubic talk about the actual mechanics of that process.

Mr. KUBIC. I wish I could.

Actually, what we do is we work very closely with the Internet service providers, so that when we get a court order, we would go to the Internet service provider. It is at that point that the questions come up, because some of the routing of the e-mail messages go out-of-state, sometimes they go through another country, and it gets very, very confusing very quickly.

We have had occasions where some of the service providers have requested conflicting-type orders. So, for instance, they were mixing up orders that would provide the content of the e-mail when, in fact, we're just simply seeking a trap and trace order. So the

people who are trying to do the job get confronted with the battery of corporate counsel, who might not have a real good understanding of the law. We engage in a little bit of an educational process in so doing.

But I think what we're saying is that there needs to be a very clear—clearly-written language in any legislation proposed, that precisely spells out the how-to, so that not only the Federal agents, but also the recipients of the order clearly understand what they are being asked to do and what the overages are.

Mr. SCOTT. Mr. Chairman, could I get an additional minute, so that Mr. Davidson could——

Mr. SMITH. Without objection, the gentlemen is recognized for an additional minute.

Mr. SCOTT. Before you respond, Mr. Davidson, if someone has an expectation of privacy on their e-mail, what limitations should we be looking for, particularly in light of the fact that trap and trace is, as I understand it—has to be issued by the judge, based on the certification of law enforcement that it is needed—the judge has no discretion—and whether or not it is possible to an e-mail without getting the content?

Mr. DAVIDSON. Well, I think this is—it highlights a very difficult problem which I was trying to get at before, about the extension of the trap and trace and pen register statute into the Internet world. The fact is that the source of destination of e-mail traffic may be much more revealing then the digits dialed on a telephone, partly because e-mail addresses are much more intimately connected to a person and an individual than a telephone, which may be used by many different people, and this especially applies to the extension of pen registers and trap and traces to finding Web URLs, resource locators, when you type in http, which is our understanding of a desire of the Justice Department, also and we have seen this in the context of the implementation of Carnivore.

I think that what you hit on is the fact we do need clarity in these laws. There's a great deal of ambiguity about how these statutes apply to the Internet, and when we add that clarity, we need to think about upping the standard a little bit. Right now, judges do not have any discretion. Once the showing is made, they are required to issue these orders. Judges should be given that discretion, to weigh the circumstances of a particular presentation, and we also need to think very carefully about this blurring line between source and destination and the content that might be embedded in a URL, where you go search for a book or something like that, and may be much more revealing than digits dialed.

Mr. SMITH. Thank you, Mr. Scott.

The gentleman from Wisconsin, Mr. Green, is recognized for his questions.

Mr. GREEN. Thank you, Mr. Chairman.

Mr. Chertoff, your opening remarks got my attention. The first example that you gave is remarkably like something that happened in my district back in northeastern Wisconsin, in which a couple that had broken up, divorced, the ex-husband was posting photos, intimate photos, of his ex-wife on the Internet and e-mailing them to places that she frequents, business and such, and we have been looking for ways to provide tools for prosecutors to deal with that

instance, which is remarkably like the one that you pointed out. What tools do you think we should be looking for? What would help you in those kinds of situations?

Mr. CHERTOFF. Well, I think this is a problem which is increasing. I think we have some very good statutes now. One of the issues we have to address, though, are statutes that couch criminality in terms of dollar value, where you have, for example, computer invasions or intrusions that do damage above a certain amount of money, and the reality is that sometimes the damage that is done cannot be quantified, but it can be, in fact, more serious than monetary damage.

I think one of the things I would like to do going forward is to sit and look comprehensively at all the statutes that cover identity theft, computer crime and make sure we have what I would call a seamless system, where we are really covering the kinds of invasions of privacy and damage that we are becoming concerned about.

Mr. GREEN. What I would like to do, if I can, is to send you a draft of what we have been working on, because we have been flailing about, trying to figure out just how to get our arms around this situation, and would welcome your thoughts and comments. Let me shift gears to Mr. Kubic and Mr. Savage. Last session, I co-authored legislation with Senator Collins which passed, dealing with the problem of fake IDs and how they were being either transmitted or marketed over the Internet, and the legislation passed and created a committee to deal with the issue of Internet fake IDs, and how their could be a cross-agency task force on the subject.

Are you aware of whether or not that task force has, in fact, been assembled and if there has been any progress on this issue?

Mr. KUBIC. Congressman, I am unaware of whether or not that specific task force has been assembled. However, the Department of Justice does host and share regular meetings that deal with the theft of—identity theft—broadly. I'm not sure if that was what you had in mind.

Mr. GREEN. One of the things that the testimony suggested last session was that about 83 percent of all fake IDs, everything from the fake IDs we often think of for underage alcohol abuse to forged passports and such, 83 percent by next year will be procured over the Internet, and for a variety of reasons, it is difficult for us to trace and block that. That was the reason for the legislation, and, as I said, it created actually a task force on that.

Mr. Savage I don't know if you're aware of whether or not that task force has been created.

Mr. SAVAGE. Congressman, as I understand it, we participate in the same task force or the same group alluded to by Mr. Kubic, and it is my understanding that suffices for the task force envisioned, but I am not 100 percent sure on that. I can say that Secret Service recognizes the problem, especially with respect to identity fraud. We have placed an agent full-time at the Federal Trade Commission to help coordinate with respect to identity fraud cases.

Mr. GREEN. If the two of you could check into it, because there was actually a coordinating committee established by this legislation signed into law last session. The law is now Public Law 106–

578, and I would appreciate any follow-up you could give us as to its status. Finally, the legislation as we originally introduced it, not all the provisions were adopted. One of the provisions that fell away would have made it illegal to knowingly produce or transfer a document that is designed for use in the production of false IDs, as opposed to just the marketing, the actual transmission of the document.

One of the reasons it was dropped is because it sort of hit the jurisdiction of a number of Committees and again has some technical challenges to it. Do you have any comments on whether or not that would be useful, or your thoughts on that type of proposal?

Mr. SAVAGE. Congressman, my response is such a thing probably would be quite useful. The limiting factor usually in such legislation is proving that intent, that it was designed to be used in the commission of a fraud, and certainly that prerequisite, that standard, is usually found in the fraud statutes for good reason. However, it would be of value to see if there would be something similar that could be substituted in that regard.

Mr. GREEN. As you may know, of the reasons that this is a growing problem is that these documents are transmitted with an easily-removed sticker on the back that says, "Not a Government document; for entertainment purposes only." Of course, when the recipient gets it, they simply peel off the sticker and they have their documents. That is why we have tried to get at this, but the intent, obviously, is the difficult issue to prove.

Mr. Kubic, I don't know if you have any thoughts on that.

Mr. KUBIC. Manufactured, false or counterfeit documents are often found in a lot of the fraud cases that we see, whether it is financial institution fraud, credit card fraud, it rivals the theft of real identities as an issue.

Mr. GREEN. Thank you.

Mr. SMITH. Thank you, Mr. Green. The gentleman from Virginia, Mr. Goodlatte, is recognized for his questions.

Mr. GOODLATTE. Thank you, Mr. Chairman. First, thank you for holding this and the continuing series of hearings on crime on the Internet.

Mr. Kubic, in your testimony, you state that difficulty with online crime is that there are no fingerprints, shoe impressions, surveillance video or photographs, money taken or witnesses, and that the evidence can be lost forever rather quickly. How does the FBI handle this problem with cyber crime investigations?

Mr. KUBIC. Well, basically, while I say that there—the evidence exists in a somewhat different form. Rather than the physical fingerprint that is left, there is, in fact, an electronic fingerprint that is most useful in establishing some of the people who are engaged in the theft, using that as an example. What happens, however is that many of the people that we look in terms of intrusions or hacking use different platforms and bounce around through the cyber world.

So while it is a different type of evidence that we are seeking, there are active steps taken by this category of criminals to hide their efforts. We have an engineering research facility at Quantico, as well as technically-trained agents in each of our field offices, who are actively engaged in the collection and preservation of evi-

dence in digital form. Additionally, the FBI has computer response teams that do things like mirroring images—mirror-image creation of seized computers, wherein we can further identify the activity of a particular suspect or subject.

Mr. GOODLATTE. Thank you.

Mr. Davidson has testified that cyber crime is more traceable than physical, real world crime. Would you disagree with that statement, and, if so, why?

Mr. KUBIC. I would not say it is more traceable at all. I think it represents a new challenge for law-enforcement investigators. Because of the nature of the evidence being so much different from what we collect in a normal crime scene, there is a need, one that is being met, I think, in part today, to retrain, to retool, and to upgrade the set of skills that the investigators have, whether they are State and local officers or Federal agents.

Mr. GOODLATTE. Go ahead, Mr. Davidson.

Mr. DAVIDSON. No. I might say that it is actually sort of—it is differently available than it is in the offline world, and that is definitely true. We support the tremendous challenge that is in front of law-enforcement officials to retool and retrain agents to be able to deal with this, these new kinds of evidence, but I think it is worth recognizing that we have heard many claims that substantial new authorities are needed because it is so difficult to find evidence online; and I think there are many reasons to believe that once—when we take on this substantial challenge of retooling ourselves, we will find that, on balance, there's actually a tremendous amount of information that's out there.

Mr. GOODLATTE. Let me get into a specific area that concerns me, and that is the distribution of obscenity or child pornography online. You have stated that powerful statutes exist to punish that distribution and I agree, but I think—and I will ask the other gentleman whether they agree or not—I think there are some gaps in that law that inhibit law-enforcement in investigating this type of behavior. Would any of you care to respond to his assertion?

Mr. CHERTOFF. Well, I think that that is a very good example of an area where some of these procedural problems that we face, legal problems, can be an impediment. I think that the actual substantive laws, for example, dealing with child exploitation, are good laws. Now, you know, Congressman, there is an issue now before the Supreme Court regarding one subset of that involving so-called virtual reality. But again we need to be able to move quickly. The people who are purveying this material, some of them are unsophisticated, but some of them are sophisticated. Some of them are overseas. By streamlining the procedures, without sacrificing privacy, I think we can add tools that will allow our investigators to be more effective.

Mr. GOODLATTE. One of the areas that concerns me, and I'm not sure what to do about it, are these online chat rooms, which are the genesis of the great deal of problems we have with predators online, with the so-called travelers who will go into these chat rooms and develop a relationship with a 12, 13, 14-year-old boy or girl and then attempt to develop that relationship, meet them.

We have a local law-enforcement agency in my district; Bedford County Sheriff's Department has Operation Blue Ridge Thunder,

which receives funds through a Federal grant program, and have been very effective in prosecuting dozens of people all over the country who, in many instances, come to Bedford with clearly malicious intent to do so, and trying to break that link, trying to make it easier for law-enforcement to do something in the chat room itself, is of interest to me.

Obviously, we have got to be concerned about the first amendment and what happens there, but do any of you have any thoughts on what can be done to criminalize the initial activity of these individuals who get online and attempt to discuss, in some instances, obscene activities online with children? Is there a constitutional prohibition on attempting to have a prohibition on adults discussing these types of thing online, with minors, for example?

Mr. CHERTOFF. Obviously, there are constitutional limits on your ability to regulate discussion, and I know that Mr. Kubic can speak to this, the Bureau has been very effective in using active investigative techniques to ferret out those people who get into those chat rooms in a predatory fashion. I think that is really a very effective tool, and I will let Tom talk about that.

Mr. KUBIC. Yes, under the Innocent Images initiative, the traveler-type cases, the cases that you have kind of defined, which means in brief that there's an individual posing as a teenager engaging in conversation, trying to either lure a young person to visit him or to be more upfront about their intentions, and then they themselves travel to another district to engage in some type of elicit activity, are the top priority of our Innocent Images investigations.

Mr. GOODLATTE. But at the point where they actually attempt to travel. I know the sheriff's department, for example, has officers that pose as 13, 14-year-olds, and do that, and it is only when they get to the point of actually attempted to have a meeting, that they attempt to prosecute; and if there were a chill, and I know first amendment folks love to hear that word chill, but if there were a chill on this type of activity, because people, if they went online and were deliberately, under some definable criminal statute, engaging in an activity that were illegal in and of itself, we could prevent this whole thing from happening in the first place. I will let you respond to that, and I would also like to hear Alan Davidson's view on that.

Mr. KUBIC. Well, I understand, you know, your position. I think it would be extremely difficult to write legislation which would cover that kind of conduct, because to a very great extent it is merely a discussion and often, you know, is this a fantasy or is there an effort to really engage in some illicit act?

Mr. GOODLATTE. But when you're dealing with a minor, does it matter if it is a fantasy or not, if an adult is engaged in that type of a discussion of activities?

Mr. DAVIDSON. Well, I would say that we really need to tread lightly here, in the sense that the distinction between speech and action has been an important one, in terms of constitutionality of these kinds of statutes, and I would just suggest——

Mr. GOODLATTE. But remember what we are talking about. These are adults with a very serious disposition. This is all part

of the intent. It is all part of the formation of a crime, and you're having people engage in very salacious discussions with kids who think it is really cool to do this with some adult who is doing it online like this.

Mr. DAVIDSON. The courts have afforded a great deal of protection to adult speech.

Mr. GOODLATTE. Even with minors?

Mr. DAVIDSON. I believe so, and I think it is a very—it is a very—the knowledge component of this was very tricky, and all I can say is I know the congressman has a record of being very concerned about these issues. I think there is a resource question.

Mr. GOODLATTE. I am very concerned about the first amendment. I'm also very concerned about children in the type of circumstances that we are defining here.

Mr. DAVIDSON. And I think that we should recognize that the Internet, in many ways, has also provided this new tool that we didn't have before, which is to bring people out, the kinds of people that you are trying to—that you would like to prosecute here—to bring them out of the dark corners of society and into places where the FBI and other law-enforcement agencies can very effectively, increasingly effectively, find them and prosecute them, and that is an effort that we should continue. But we need to do——

Mr. GOODLATTE. Not if they can—as long as they never have that meeting with the individual, you're telling me that not only are we bringing them out of the dark corners, but we're giving them a forum in which to engage in this activity in a protected way that they never had before, and it is causing an explosion of difficulty in this area.

Mr. DAVIDSON. And perhaps a new way to find them. No doubt that this is a problem and that more work needs to be done on the enforcement side.

Mr. SMITH. Thank you, Mr. Goodlatte.

The gentleman from Virginia will be recognized for an additional question.

Mr. SCOTT. Yes, Mr. Chertoff, you mentioned virus crimes. Should we be considering anything to help on the jurisdiction of the crime; the perpetrator may be traveling with a laptop; the victim may have a laptop? How do you figure out what the jurisdiction of the crime is, or has that been a problem?

Mr. CHERTOFF. Well, I think that is a species of the same kind of problem we talked about earlier, with pen registers and trap and trace orders. Typically, for example, if you are intercepting data in real-time and you're going to get what we call a title III authorization from a judge, again there have been issues historically about going to the right jurisdiction. If I want to tap a particular phone, I go to a judge, I get a title III order, let's say in New Jersey. I know the phone is in New Jersey. Even in the area of cell-phones now, we have developed laws and techniques that allow us to basically attach the order to the traveling phone. And I think we want to be able to do the same thing with respect to traveling laptops.

Again, the idea is not to dilute the protection, the substantive protection of privacy under the law. The idea is to eliminate the problem of geographic limitations on judicial orders. So one of the

things I think we want to do is essentially create one-stop shopping for these kinds of orders.

Mr. SCOTT. I'm talking about the prosecution. What court do you go in to get the indictment?

Mr. CHERTOFF. Well, typically the general rule with respect to venue in criminal cases is anywhere the crime occurs, so any place somebody traveled in the course of committing an illegal act, if the illegal act occurred over the Internet, would be the place that we could bring the case.

Mr. SCOTT. Do you have to prove jurisdiction? I know in State court, you have to prove the crime was committed within the State. Do you have a jurisdictional part of the prosecution where you have to show that the crime was committed in State where you may not know where the guy was?

Mr. CHERTOFF. You do. You do have to prove venue, because you have to bring the case in the appropriate venue. And it may be, Congressman, that what you're suggesting is something worth thinking about, which is whether we ought to create a venue provision that allows us to prosecute crimes in certain designated places, whether or not the person was actually traveling in that place or broadcasting while they were traveling.

I could certainly envision proof problems, for example, in showing when—you know, where someone was at the time they transmitted a particular message, and perhaps we want to make sure in the law that we can adequately address these, where the service provider is located, where the recipient is at some other place. I think that is worth looking at.

Mr. SCOTT. Mr. Davidson, do you want to——

Mr. DAVIDSON. Well, I would just indicate that, of course, there are going to be issues here on the user side, as well, which is that users don't necessarily know where all of their communications are going, who they are necessarily using when they're on the Internet. Your ISP may be routing communications all over the place, and I think—which just demonstrates the difficulty here also on the user side, of finding out that you may be subject to an order that has been issued across the country, that you may not necessarily have knowledge of, that you may have a difficulty in terms of answering or defending.

In many of these cases, of course, you never have notice of this. But I think there are some mitigating difficulties on the user end that need to be worked out, also.

Mr. SMITH. Thank you, Mr. Scott. Before we adjourn, I do want to say, and the witnesses might be interested in it, as well, and it has been mentioned by one witness, and the audience may be interested in knowing that we are having our third and last hearing on cyber crime this coming Thursday, day-after-tomorrow, at 10 o'clock in the morning, and that will conclude our series; and, in fact, so far as I know, we will have had more hearings on that subject than on any other subject this year.

So that is the importance we attach to it and that is how serious we are about trying to be helpful to all of you all, law-enforcement and those interested in privacy concerns, as well.

Mr. Chertoff, I just want to tell you, if you have been head of the Criminal Division for less than 2 weeks, you sounded like a veteran today. So you're off to a good start.

Mr. CHERTOFF. Thank you, Mr. Chairman.

Mr. SMITH. We thank all the witnesses. We appreciate their testimony and their expertise, and we stand adjourned.

[Whereupon, at 5:11 p.m., the Subcommittee was adjourned.]

FIGHTING CYBER CRIME: EFFORTS BY PRIVATE BUSINESS INTERESTS

THURSDAY, JUNE 14, 2001

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CRIME,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to call, at 10:10 a.m., in Room 2237, Rayburn House Office Building, Hon. Lamar Smith, Chairman of the Subcommittee, presiding.

Mr. SMITH. Since we are expecting votes in about 45 minutes, and because it would interrupt us if we are not finished, we are going to try to proceed fairly quickly.

I also want to mention that the Ranking Member, Bobby Scott, is testifying before another Committee, or he would be here now, and we still expect him shortly. Nevertheless, I'm going to recognize myself for an opening statement, and other Members if they have them, and then we'll proceed.

This is the third and last hearing in a series. I expect this hearing to assist Congress in deciding how to reduce cyber crime.

At the prior two hearings, Federal and local law enforcement officials told us that better training, additional resources, and increased cooperation and coordination are needed. Crime is still crime, whether it occurs on the street or on the Web.

While other crime rates continue to drop, cyber crime is dramatically increasing. According to law enforcement officials, cyber crime causes billions of dollars in losses every year. For example, last May one computer virus disrupted the communications of hundreds of thousands of computers, causing losses estimated in the billions of dollars. And in March of this year the FBI issued a warning that an organized group of Russian hackers had stolen more than a million credit card numbers from companies' databases.

In addition, the witnesses testified that the statutes governing processes and procedures to investigate and prosecute cyber crime must be updated.

Today the Subcommittee on Crime will hear testimony from representatives of private industry on how they deal with the growing problem of cyber crime, and also on their recommendations for how Congress should reduce cyber crime.

Businesses are losing billions of dollars from cyber crime activities that range from fraud to piracy to sabotage. The Internet has fostered an environment where hackers retrieve private data for amusement, individuals distribute software illegally, and viruses circulate with the sole purpose of debilitating computers.

In confronting this issue, the business community faces a dilemma. Do they report cyber crime at the risk of losing the public's confidence in their ability to protect customer information, or do they fail to act and risk losses and repeat attacks?

Legislation alone cannot adequately combat the prevalence of cyber crime we face today. Private industry want to protect their businesses and customers provide the first line of defense. The private sector is usually ahead of Government on the latest technology, and must be willing to cooperate with law enforcement agencies. Technology holds the key to the future, and private businesses are leading the way in innovation and products, but if left unchecked, cyber crime will stifle that progress.

I hope to hear from the witnesses on how their companies and businesses are working to reduce cyber crime. I would also like to hear about their concerns and suggestions regarding legislation.

[The prepared statement of Mr. Smith follows:]

PREPARED STATEMENT OF THE HONORABLE LAMAR SMITH, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

This is the third and final hearing in a series on cyber crime. I expect that, as the other two hearing have done, this hearing will offer valuable insight for Congress to assist in the country's efforts against cyber crime.

At the prior two hearings, federal and local law enforcement officials told us that better training, additional resources and increased cooperation and coordination are needed.

The witnesses provided us with examples of successful cooperation between state and local law enforcement. They all agreed that Congress should assist in establishing more regional computer forensic laboratories as a way to pool resources and enhance coordination. In addition, the law enforcement witnesses testified that the statutes governing processes and procedures to investigate and prosecute cyber crime must be updated.

The Subcommittee also heard from the privacy and civil rights community. The witness urged the Subcommittee to consider privacy issues in drafting any legislation, which we will do as a matter of course.

Today, the Subcommittee on Crime will hear testimony from representatives of private industry regarding their efforts to deal with the growing problem of cyber crime. Businesses are losing millions of dollars from cyber crime activities that range from intrusions to piracy.

In confronting this issue, the business community faces a dilemma. Do they report cyber crime at the risk of losing the public's confidence in their ability to protect customer information? Or, do they not report the event and risk additional losses in money and business and perhaps repeat attacks? In making this decision, businesses should remember blackmailers rarely ask for one lump sum and bullies thrive on the vulnerable.

With so much at stake, businesses have a strong incentive to prevent cyber crime. In addition to relying on the criminal laws, businesses are cooperating with federal, state and local governments and law enforcement to share information and educate the community to reduce vulnerabilities.

Legislation, alone, cannot adequately combat the level of cyber crime we face today. Private industry that wants to protect their businesses and their customers provide the first line of defense. The private sector will always be ahead of government on the latest technology, and must be willing to cooperate with each other and with law enforcement.

I hope to hear from the witnesses on exactly how their companies and businesses are working towards better cooperation. I also would like to hear about there concerns and suggestions regarding legislation and thank them for their participation.

At this time, I recognize Bobby Scott, the ranking Member, for an opening statement.

Mr. SMITH. I'll recognize Mr. Green, if he has an opening statement or comments.

Mr. GREEN. No.

Mr. SMITH. And if not, then we'll proceed and look forward to hearing from our witnesses. They are Mr. Harris N. Miller, President, Information Technology Association of America; Mr. Robert Chesnut, Vice President and Deputy General Counsel, eBay, Incorporated; Mr. Robert Kruger, Vice President for Enforcement, Business Software Alliance; and the Honorable Dave McCurdy, President, Electronic Industries Alliance, a former colleague of ours in Congress.

We welcome you all, and Mr. Miller, we'll start with you.

STATEMENT OF HARRIS N. MILLER, PRESIDENT, INFORMATION TECHNOLOGY ASSOCIATION OF AMERICA

Mr. MILLER. Thank you very much, Chairman Smith. It's a great honor to be here before the Subcommittee, and to be working with you again. You've managed to graduate from that immigration merry-go-round to a more interesting, different kind of challenge here as the Chairman of this Subcommittee.

I commend the Subcommittee for holding a series of hearings, and recognizing the cyber crime issue, as you pointed out in your opening statement, is an enormous challenge, and that industry leadership, in meaningful partnership with Government, is essential.

The stakes involved are enormous. Information technology currently represents over 6 percent of the global domestic product, and over 8 percent of US GDP, according to Digital Planet 2000, a study released last year by the World Information Technology and Services Alliance. In addition, the IT industry has a particular challenge, because not only are we a vertical industry, as is health care or transportation or retail, for example, we're also a horizontal industry in this Internet world, underlying all those other vertical industries. So we have a double challenge, to protect our own systems, and also, of course, our customers' systems.

Cyber crime places the digital economy at risk, but too many times the assumption is made that fighting cyber crime can be done with technology alone. That is wrong. Just as the best alarm system will not protect a building if the alarm code falls into the wrong hands, a network will not be protected if the passwords are given out freely. Failures in the process and people part of the cyber crime solution may in fact be a factor in the majority of the problems we see.

The business marketplace is responding to the technology component of the equation. Our customers demand it, and therefore, IT companies supply it. However, the processes and people element tend to be more problematic elements of the challenge. The two are closely linked. From a strategic point of view, the challenge is to make information security a top priority issue for CEOs, for Government officials, and for leaders in the non-governmental sector. Moving from platitudes to practical action requires the sustained commitment of senior management in both the public and private sectors. Industry and Government must share the view that given the nation's extensive dependence on information systems, information security equates to economic security. Partnership and outreach are critical to success. We must work across industry and in-

dustry with Government. Protecting our infrastructure is a collective responsibility, not just the IT community's role.

ITAA itself is working on multiple fronts to improve the current mechanisms for combatting threats and responding to attacks. Elements of our plan internally include information sharing, awareness, education, training, best practices, research and development, and international cooperation.

In the brief time this morning, I will just focus on one of these, namely information sharing. As you pointed out in your opening statement, Mr. Chairman, sharing information about corporate information security practices is very difficult. Companies are understandably reluctant to share sensitive proprietary information about prevention practices, intrusions and actual crimes, with either Government agencies or competitors. Gimbel's doesn't like to tell Macy's. Information sharing is a risky proposition with often less than clear benefits. No company wants information to surface that they had given in confidence that may jeopardize their market position, strategies, customer base or capital investments.

Public policy factors can also be a barrier. One of the obstacles is the Freedom of Information Act. Companies worry that if information sharing with Government really becomes a two-way street, FOIA requests for information they have provided to an agency could prove embarrassing or costly. We are working with Congressman Tom Davis and Senator Bob Bennett, and other key players on legislation to address this concern. There's also a concern about antitrust, about sharing information leading to antitrust violations. We've been in dialog with the Department of Justice, and we believe this issue can be partially addressed through letters from the Department of Justice, but it is something we need to take a closer look at.

The IT industry has adopted several formal approaches to the information-sharing challenge. For instance, in January of 2001, 19 of the Nation's leading high-tech companies announced the formation of a new Information Technology—Information Sharing Analysis Center, the IT ISAC, to cooperate on cyber security issues. The objective of the IT ISAC is to enhance the availability, confidentiality, and integrity of network information systems. It is a non-for-profit organization that will allow information sharing, including the possibility of anonymous information sharing within the IT industry, and ultimately between various segments of the industry, and ultimately between industry and Government. The IT ISAC has made excellent progress in the 6 months since its founding, and is in the process of being formally "stood up."

Another example is the Partnership for Critical Information Security. This partnership, which was started under the previous Administration and continues to be supported by Secretary of Commerce Don Evans in the current Administration, brings together key sectors of our economy to work across sectors, so that the financial sector, the retail sector, the health sector, the energy sector, the IT sector and others, share information. Again, this is not a stove-pipe issue, and they must work together. The PCIS had a major meeting in Washington, D.C. in March, which was addressed by the National Security Advisor, Dr. Rice, and that meeting

helped to pull together and coalesce this partnership. We now have formal mechanisms being developed to provide information sharing.

In sum, Mr. Chairman, the challenge is large so the achievement will be formidable. While cyber crime will never be eliminated, it can be contained through effective information security products, intelligent practices, and suitably trained people. But none of this will occur, again I repeat, without leadership from the top, both in the private sector and in Government and collaboration between the two.

ITAA is proud to do its part. Thank you. And I welcome the opportunity to answer any questions the Subcommittee may have.

[The prepared statement of Mr. Miller follows:]

PREPARED STATEMENT OF HARRIS N. MILLER

INTRODUCTION

Chairman Smith and Members of the Subcommittee, thank you for inviting me here to testify today on cyber crime. My name is Harris N. Miller, and as President of the largest information technology trade association, the *Information Technology Association of America* <http://www.itaa.org/>, I am proud that ITAA has emerged as the leading association on the issue of information security. ITAA represents over 500 corporate members. These are companies that have a vested economic interest in assuring that the public feels safe in cyberspace; in the United States, most of the Internet related infrastructure is owned and operated by the private sector.

I am also President of the *World Information Technology and Services Alliance* <http://www.witsa.org>, a consortium of 41 global IT associations from economies around the world, so I offer a global perspective. ITAA also houses the *Global Internet Project* <http://www.gip.org/>, an international group of senior executives committed to fostering continued growth of the Internet, which is spearheading an effort to engage the private sector and governments globally on the Next Generation Internet and related security and reliability issues.

I commend this Subcommittee for holding a series of hearings on cyber crime and recognizing that to solve this enormous challenge, industry leadership, in meaningful partnership with government, is essential.

The stakes involved are enormous. Information technology represents over 6 percent of global gross domestic product (GDP), a spending volume of more than $1.8 trillion, and over 8 percent of US GDP, according to *Digital Planet 2000*, a report released last year by WITSA. According to the *US Department of Commerce*, IT accounted for approximately one-third of the nation's real economic growth from 1995 to 1999. Despite the current slowdown, IT-driven productivity increases have enabled our country to have what many economists thought we could not have: high growth, low unemployment, low inflation, and growth in real wages.

The IT industry's importance to the economy goes beyond the numbers I just recited, however, because the IT industry is not only a vertical industry-such as financial services or health care-it is also a horizontal industry whose technology and services under gird all the other industry sectors. For instance, the failure of a particular IT company to meet the information security challenge not only hurts that company's bottom line, it also hurts the bottom line of companies to which it provides software or IT services.

ECONOMY AT RISK

Cyber crime places the digital economy at risk. Just as the reality or threat of real crime can drain the economic vitality of neighborhoods, cities and even nations, so to can the reality or threat of crimes committed online against people and property shutter businesses and cause an otherwise motivated digital public to break their Internet connection.

Cyber crime falls into several categories. Most incidents are intended to disrupt or annoy computer users in some fashion. Distributed denial of service (DoS) attacks crash servers and bring down websites through the concerted targeting of thousands of email messages to specific electronic mailboxes. Viruses and other malicious code introduce phantom computer software programs to computers, designed intentionally to corrupt files and data. Other online intrusions are conducted to deface websites, post political messages or taunt particular groups or institutions. Even though no one stands to profit, damages caused by such attacks can run from the

trifling to the millions of dollars. What motivates these attackers? Hackers may view the attack as a technology challenge, may be seeking to strike a blow against the establishment, may be looking for group acceptance from fellow hackers, or may be just indulging themselves in a perverse thrill.

Other cyber criminals are more material guys and gals. They hope to profit from their intrusions by stealing valuable or sensitive information, including credit card numbers, social security numbers, even entire identities. Targets of opportunity also include trade secrets and proprietary information, medical records, and financial transactions.

For some cyber criminals, the Internet is a channel for the dissemination of child pornography and a tool used in the furtherance of other crimes against children and adults. These crimes include fraud, racketeering, gambling, drug trafficking, money laundering, child molesting, kidnapping and more.

Cyber terrorists may seek to use the Internet as a means of attacking elements of the physical infrastructure, like power stations or airports. As we have seen in the Middle East, cyber terrorists encouraging political strife and national conflict can quickly turn the Internet into a tool to set one group against another and to disrupt society generally.

Another class of cyber criminal and, unfortunately, the most common is the insider who breaks into systems to eavesdrop, to tamper, perhaps even to hijack corporate IT assets for personal use. These could be employees seeking revenge for perceived workplace slights, stalking fellow employees, looking for the esteem of peers by unauthorized "testing" of corporate security, or other misguided individuals.

Regardless of category, the threat is real. *A recent study* produced by Asta Networks and the University of California San Diego monitored a tiny fraction of the addressable Internet space and found almost 13,000 DoS attacks launched against over 5000 targets in just one week. While most targets were attacked only a few times, some were victimized 60 or more times during the test period. For many small companies, being knocked off the Internet for a week means being knocked out of business for good.

The Computer Security Institute/FBI also documents the problem in a widely reported study on computer breaches. This year's survey of 538 respondents found 85 percent experiencing computer intrusions, with 64 percent serious enough to cause financial losses. Estimated losses from those willing to provide the information tallied $378 million, a 43 percent increase from the previous year.

A nationwide public opinion poll released last year by ITAA and EDS showed that an overwhelming majority of Americans, 67 percent, feel threatened by or are concerned about cyber crime. In addition, 62 percent believe that not enough is being done to protect Internet consumers against cyber crime. Roughly the same number, 61 percent, say they are less likely to do business on the Internet as a result of cyber crime, while 33 percent say crime has no effect on their e-commerce activities. The poll of 1,000 Americans also revealed that 65 percent believe online criminals have less of a chance of being caught than criminals in the real world, while only 17 percent believe cyber criminals have a greater chance of being caught.

BATTLING CYBER CRIME: INFORMATION SECURITY

Information security is the multifaceted discipline that counteracts cyber crime. Information security—or InfoSec—deals with cyber crime prevention, detection and investigation. How do we achieve information security?

INFORMATION SECURITY IS BUILT FROM TECHNOLOGY, PROCESSES AND PEOPLE

Too many times, the assumption is made that fighting cyber crime can be done with technology alone. That is wrong. Just as the best alarm system will not protect a building if the alarm code falls into the wrong hands, a network will not be protected if the passwords are given out freely. Failures in the "process and people" part of the cyber crime solution may, in fact, be the majority of the problems we see.

The marketplace is responding to the technology component of this equation. Our customers demand it and, therefore, ITAA members supply it. Beyond that simple yet effective commercial dynamic, we also see market pressures beginning to coalesce. As cyber crime becomes more common and more pervasive, we will hear a building chorus of demand for information security solutions from insurance firms, health care providers, financial services companies, utilities, and the public at large.

The degree to which such products are necessary is in large part determined by the level of risk incurred. In most cases, for instance, security levels required to protect an email application would not be as robust as those protecting electronic funds transfer. Organizations must be able to select the technology solution that is ade-

quate to the job at hand. The marketplace must have the commercial incentive to deploy a variety of technology solutions, be they password protection, encryption, firewalls, biometrics or other means.

Processes and people tend to be the more problematic elements of the policy puzzle. The two are closely linked. From a strategic point of view, the challenge is to make information security a top priority issue. Moving from platitudes to practical action requires the sustained commitment of senior management.

The goal is to embed information security in the corporate culture. That is not always easy to do. CEO's want their IT systems to be as fast as a Maserati—but as safe as a Brinks truck. Whenever tradeoffs arise, the bias is towards speed, not safety. The challenge for the IT sector and its customers working together is to provide security at the speed of business.

Organizations must be willing to invest in the development of comprehensive security procedures and to educate all employees—continuously. The primary focus of improving processes and changing behaviors is inside the enterprise. However, the scope of the effort must also take into account the extended organization-supply chain partners, subcontractors, customers, and others that must interact on a routine basis.

ORGANIZATIONS MUST ALSO BE PREPARED TO COOPERATE WITH LAW ENFORCEMENT

Unfortunately, companies often feel that the disruption to operations and potential damage to reputation outweigh the benefits of such cooperation. Until the private sector feels that it can do so on a reasonable basis, hackers and cyber criminals will have a significant advantage. ITAA and the Department of Justice conducted a series of executive level meetings and conferences last year, including participation by then Attorney General Janet Reno, to work towards a new dialogue on this issue. More such events will be held later this year. Companies can move this process along by working through trade associations and groups like the Partnership for Critical Infrastructure Security <http://www.pcis-forum.org>, to achieve the necessary balance of public and private interests.

The challenge of processes and people is not a concern for the private sector alone. The federal government must play a significant role as well. The Administration, for instance, must bring substantial leadership to the information security arena and help raise the nation's level of awareness about cyber attacks and preventative measures. A major part of this message must be that, given the nation's extensive dependence on information systems, *information security means economic security*.

The responsibility is both national and international. The U.S. has critical defense and economic relationships around the globe. A breakdown in any link of this chain can have cascading consequences. It is, therefore, incumbent on the U.S. government to accept its global information security role and educate foreign governments as to the nature of the threat and how to respond to it. Industry stands ready to work with multinational organizations and NGOs to help in this process.

INDUSTRY PLAN FOR CYBER SECURITY

ITAA and its members have been working to execute a multi-faceted plan designed to improve U.S. cooperation on issues of information security. However, Mr. Chairman, we would all be remiss if we believed it was just the IT industry that must cooperate within its own industry—we must work cross industry, and industry with government. Protecting our infrastructure is a collective responsibility, not just the IT community's role.

We are working on multiple fronts to improve the current mechanisms for combating threats and responding to attacks through our role as a Sector Coordinator for the Information and Communications sector, appointed by the U.S. Department of Commerce. Through ITAA's InfoSec Committee, our member companies also are exploring joint research and development activities, international issues, and security workforce needs. Elements of the plan include Information Sharing, Awareness, Education, Training, Best Practices, Research and Development, and International Coordination.

INFORMATION SHARING: Sharing information about corporate information security practices is inherently difficult. Companies are understandably reluctant to share sensitive proprietary information about prevention practices, intrusions, and actual crimes with either government agencies or competitors. Information sharing is a risky proposition with less than clear benefits. No company wants information to surface that they have given in confidence that may jeopardize their market position, strategies, customer base, or capital investments. Nor would they risk voluntarily opening themselves up to bogus but costly and time-consuming litigation. Releasing information about security breaches or vulnerabilities in their systems pre-

sents just such risks. Negative publicity or exposure as a result of reports of information infrastructure violations could lead to threats to investor—or worse—consumer confidence in a company's products. Companies also fear revealing trade secrets to competitors, and are understandably reluctant to share such proprietary information. They also fear sharing this information, particularly with government, may lead to increased regulation of the industry or of electronic commerce in general.

Public policy factors also act as barriers to industry information sharing. One of the obstacles is the Freedom of Information Act (FOIA). Companies worry that if information sharing with government really becomes a two-way street, FOIA requests for information they have provided to an agency could prove embarrassing or costly. FOIA requests place the private sector's requirement for confidentiality at odds with the public sector's desire for sunshine in government information. We are working with Congressman Tom Davis (R-VA), Senator Robert Bennett (R-UT), and other key players on legislation to meet this concern.

Anti-trust concerns are a second potential legal hurdle to information sharing. Fortunately, such risks appear small. The antitrust laws focus on sharing information concerning commercial activities. Information Sharing Advisory Centers (ISACs) should be in compliance with the antitrust laws because they are not intended to restrain trade by restricting output, increasing prices, or otherwise inhibiting competition, on which the antitrust laws generally focus. Rather, ISACs facilitate sharing of information relating to members' efforts to enhance and to protect the security of the cyber infrastructure, so the antitrust risk of such exchange is minimal. The Justice Department has also indicated that there are minimal antitrust concerns involving properly structured joint industry projects for dealing with externalities. An entity created to share information regarding common threats to critical infrastructure should fall into this category.

Given the changing nature of the cyber crime threat and in spite of the many business, operational and policy hurdles standing in the way, many companies in the private sector recognize the need to have formal and informal information sharing mechanisms. Internet Service Providers are an example of the latter circumstance. Because these firms provide networking capability commercially, these businesses often have extensive network security expertise. Such firms act as virtual Information Sharing and Analysis Centers, gathering information about detected threats and incursions, sanitizing it by removing customer specific data, and sharing it with customers.

The IT industry has adopted a formal approach to the information sharing challenge. In January 2001, nineteen of the nation's leading high tech companies announced the formation of a new Information Technology Information Sharing and Analysis Center (IT-ISAC) to cooperate on cyber security issues. The objective of the IT-ISAC is to enhance the availability, confidentiality, and integrity of networked information systems. The group has made excellent progress in the six months since its founding and is in the process of being formally "stood up," although information sharing is already beginning to take place within this ISAC.

The IT-ISAC is a not-for-profit corporation that will allow the information technology industry to report and exchange information concerning electronic incidents, threats, attacks, vulnerabilities, solutions and countermeasures, best security practices and other protective measures. Its internal processes will permit information to be shared anonymously. The organization is a voluntary, industry-led initiative with the goal of responding to broad-based security threats and reducing the impact of major incidents. Membership in the IT-ISAC is open to all U.S.-based information technology companies. It will offer a 24-by-7 network, notifying members of threats and vulnerabilities. The group also is clear on what is will not undertake. Excluded activities include standards setting, product rating, audits, certifications or dispute settlement. Similarly, the IT-ISAC is not a crime fighting organization. The nineteen Founding Member companies of the IT-ISAC, all represented at the announcement, are AT&T, Cisco Systems, Computer Associates, CSC, EDS, Entrust Technologies, Hewlett-Packard Company, IBM, Intel Corporation, KPMG Consulting, Microsoft Corporation, Nortel Networks, Oracle Corp., RSA Security, Securify Inc., Symantec Corporation, Titan Systems Corp., Veridian and VeriSign, Inc.

The group plans to evolve its information sharing activities over time, starting with IT companies and then moving across sectors. It is also expected that the ISAC will enable sensitive information to be shared between industry and government. But that sharing must be a two-way street, if it is going to be effective.

The Software Engineering Institute's CERT Coordination Center plays an information sharing role for numerous industries. The oldest and largest of information sharing programs, CERT is a Federally funded research and development center at Carnegie Mellon University in Pittsburgh. The organization gathers and dissemi-

nates information on incidents, product vulnerabilities, fixes, protections, improvements and system survivability. The organization strives to maintain a leak proof reputation while collecting thousands of incident reports yearly. These could be anything from a single site reporting a compromise attempt to a virus with worldwide impact.

The IT-ISAC is specifically designed to support the IT industry in this country. Other ISACs have been formed in the financial services and telecommunications industries. And I would like to mention two other groups that play an important information sharing role. The Partnership for *Critical Infrastructure Security* provides a venue for organizations from numerous industries to pool their knowledge and experience about information infrastructure risks and protections. PCIS also examines critical interdependencies among infrastructure providers and seeks common solutions to risk mitigation. *The Partnership for Global Information Security* <http://www.pgis.org/> provides a forum for executives from both the public and private sector in economies around the world to share information about InfoSec topics. PGIS members are focused on five areas for collaboration: sound practices, workforce, research and development, cyber crime and law enforcement and public policy. ITAA is proud to have played a leadership role in the formation of both organizations, and I sit on the Boards of Directors of both.

AWARENESS: ITAA and its member companies are raising awareness of the issue within the IT industry and through partnership relationships with other vertical industries, including finance, telecommunications, energy, transportation, and health services. We are developing regional events, conferences, seminars and surveys to educate all of these industries on the importance of addressing information security. An awareness raising campaign targeting the IT industry and vertical industries dependent on information such as the financial sector, insurance, electricity, transportation and telecommunications is being overlaid with a targeted community effort directed at CEOs, end users and independent auditors. The goal of the awareness campaign is to educate the audiences on the importance of protecting a company's infrastructure, and instructing on steps they can take to accomplish this. The message is that information security must become a top tier priority for businesses and individuals.

EDUCATION: In an effort to take a longer-range approach to the development of appropriate conduct on the Internet, the Department of Justice and the Information Technology Association of America have formed the *Cybercitizen Partnership*. Numerous ITAA member companies and recently the Department of Defense have joined this effort. The Partnership is a public/private sector venture formed to create awareness in children of appropriate on-line conduct. This effort extends beyond the traditional concerns for children's safety on the Internet, a protective strategy, and focuses on developing an understanding of the ethical behavior and responsibilities that accompany use of this new and exciting medium. The Partnership is developing focused messages, curriculum guides and parental information materials aimed at instilling a knowledge and understanding of appropriate behavior on-line. The Partnership hosted a very successful event last fall at Marymount University in Northern Virginia that brought together key stakeholders in this area. Ultimately, a long range, ongoing effort to insure proper behavior is the best defense against the growing number of reported incidents of computer crime. The Cybercitizen website has received over 600,000 hits in the past year.

TRAINING: ITAA long has been an outspoken organization on the impact of the shortage of IT workers—whether in computer security or any of the other IT occupations. Our groundbreaking studies on the IT workforce shortage, including the latest, "*When Can You Start*," have defined the debate and brought national attention to the need for new solutions to meet the current and projected shortages of IT workers. We believe it is important to assess the need for and train information security specialists, and believe it is equally important to train every worker about how to protect systems.

We have planned a security skills set study to determine what the critical skills are, and will then set out to compare those needs with courses taught at the university level in an effort to determine which programs are strong producers. We encourage the development of "university excellence centers" in this arena, and also advocate funding for scholarships to study information security. We commend the Administration and Congress for supporting training more information security specialists.

The challenge to find InfoSec workers is enormous, because they frequently require additional training and education beyond what is normally achieved by IT workers. Many of the positions involving InfoSec require US citizenship, particularly those within the federal government, so using immigrants or outsourcing the projects to other countries is not an option.

BEST PRACTICES: We are committed to promoting best practices for information security, and look to partners in many vertical sectors in order to leverage existing work in this area. In addition, our industry is committed to working with the government—whether at the federal, state or local levels. For example, we are working with the Federal Government's CIO Council on efforts to share industry's best information security practices with CIOs across departments and agencies. At the same time, industry is listening to best practices developed by the government. This exchange of information will help industry and government alike in creating solutions without reinventing the wheel.

While we strongly endorse best practices, we strongly discourage the setting of "standards." Why?

Broadly, the IT industry sees standards as a snapshot of technology at a given moment, creating the risks that technology becomes frozen in place, or that participants coalesce around the "wrong" standards. Fighting cyber crime can be thought of as an escalating arms race, in which each time the "good guys" develop a technology solution to a particular threat, the "bad guys" develop a new means of attack. So to mandate a particular "solution" may be exactly the wrong way to go if a new threat will soon be appearing.

It is also critical that best practices are developed the way much of the Internet and surrounding technologies have progressed—through "de facto" standards being established without burdensome technical rules or regulations. While ITAA acknowledges the desire within the Federal government to achieve interoperability of products and systems through standard-setting efforts, the reality is that the IT industry can address this simply by responding to the marketplace demand. The marketplace has allowed the best technologies to rise to the top, and there is no reason to treat information security practices differently.

RESEARCH AND DEVELOPMENT: While the information technology industry is spending billions on research and development efforts—maintaining our nation's role as the leader in information technology products and services—there are gaps in R&D. Frankly, for industry, more money is frequently spent on "D"-development-then "R"-long-term research. Government, mainly in the Department of Defense, focuses its information security R&D spending on defense and national security issues. We believe that between industry's market-driven R&D and government's defense-oriented R&D projects, gaps may be emerging that no market forces or government mandates will address. Government funding in this gap-bringing together government, academia and industry—is necessary.

INTERNATIONAL: In our work with members of the information technology industry and other industries, including financial services, banking, energy, transportation, and others, one clear message constantly emerges: information security must be addressed as an international issue. American companies increasingly are global corporations, with partners, suppliers and customers located around the world. This global business environment has only been accented by the emergence of on-line commerce—business-to-business and business-to-consumer alike.

Addressing information security on a global level clearly raises questions. Many within the defense, national security and intelligence communities rightly raise concerns about what international actually means. Yet, we must address these questions with solutions and not simply ignore the international arena. To enable the dialogue that is needed in this area, ITAA and WITSA conducted the first Global Information Security Summit in Fall 2000. This event brought together industry, government and academia representatives from around the world to begin the process of addressing these international questions. A second Summit is planned for later this year to continue the dialogue. The governmental international linkages must be strengthened—and not just among the law enforcement and intelligence communities. Government ministries around the world involved in economic issues—such as our own Department of Commerce—need to be key players.

HOW GOVERNMENT CAN HELP

In many ways, solutions to information security challenges are no different than any other Internet-related policy issue. Industry leadership has been the hallmark of the ubiquitous success of our sector. Having said that, we also believe that government has several roles to play in helping achieve information security and combating cyber crime:

- First and foremost, like a good physician practicing under the Hippocratic oath, do no harm. Excessive or overly broad legislation and subsequent regulation crafted in a rapidly changing technology environment is apt to miss the mark and likely to trigger a host of unintended consequences. In many instances, existing laws for crimes in the physical world are adequate to ad-

dress crimes conducted in cyberspace. New legislation should always be vetted for circumstances that single out the Internet for discriminatory treatment.

- Practice what you preach. The rules of technology, process and people apply equally to the public sector. The U.S. government must lead by example in preventing intrusions into agency websites, databanks and information systems. Leadership in this area means substantial investments of new money in information security technology and services. Responding to the issue by reallocating existing dollars from current programs is robbing Peter to pay Paul and likely to play out at the expense of the American public and their confidence in e-government. It also means insisting that government agencies implement rigorous information security processes and practice them on a daily basis. Making InfoSec part of the corporate culture will require extensive senior management commitment.
- Reach out to international counterparts for crucial discussion of cyber security, and in particular, how to most constructively and effectively enforce criminal law in the increasingly international law enforcement environment fostered by the Internet and other information networks. The Council of Europe draft Convention on Cyber Crime, which, as the first such attempt to create an international convention in this area, has become a central subject of debate. It is no secret that the private sector has expressed significant concerns about several aspects of the treaty. When governments engage in the development of cyber crime legislation or participate in international organizations on this issue, government should ensure that the process is inclusive of industry, civil society and the appropriate ministries that represent these constituencies. Governments should also match the private sector's efforts to secure their information systems swiftly, robustly, and continuously.
- Bring leadership to bear through existing structures and establish an InfoSec Czar position similar to the role played by John Koskinen during the Year 2000 date rollover. With minimal staff, but strong backing from the President, Mr. Koskinen was able to have substantial influence on both the governmental and private sector efforts in Y2K. ITAA, its members and the IT industry continue to work hard to develop collegial and constructive relationships with the leadership and staff of the Critical Information Assurance Office (CIAO), the Commerce Department (DOC), the National Institute of Standards and Technology (NIST), and the Critical Information Infrastructure Assurance Program Office (CIIAP) at NTIA, as well as the National Security Council (NSC), Department of Justice (DOJ), Department of Energy, the National Information Protection Center (NIPC), and the National Security Agency (NSA).
- Funding will also help in the areas of workforce development and research. We have a critical shortage of information technology professionals generally and information security specialists specifically. In general, we support legislation to increase the number of appropriately skilled workers in this critical area. We also support additional R&D funding.

CONCLUSION

Society's reliance on information technology will only increase over time. Ultimately, the level of information security we achieve will go far in defining our level of economic security. Market forces will push us to this inevitable conclusion. These forces will include:

- Insurance companies seeking to control and assess the risk of cyber crime related losses;
- Banks seeking to assure that Internet-dependent businesses have mitigated InfoSec related risks;
- Shareholders insisting that their equity be protected through executive level attention to information security;
- Medical establishments that must assure the absolute privacy of individually identifiable patient records; and
- Critical suppliers needing to assure unimpeded flow of goods and services to plants and factories.

The challenge is large, so the achievement will be formidable. While cyber crime may never be eliminated, it can be contained through effective information security

products, intelligent practices and suitably trained people. Industry and government have important roles to play in achieving this purpose.

The Information Technology Association of America is proud to do its part.

Thank you and I welcome any questions from the Committee.

Mr. SMITH. Thank you, Mr. Miller.

Mr. Chesnut.

STATEMENT OF ROBERT CHESNUT, VICE PRESIDENT AND DEPUTY GENERAL COUNSEL, eBAY, INCORPORATED

Mr. CHESNUT. Mr. Chairman, thank you for inviting eBay here this morning to talk a little bit about what eBay does to fight cyber crime.

Before I talk about eBay's efforts, I'd like to put some of our efforts in context with some numbers, because we certainly hear a lot of numbers about online auction fraud and complaints of different Government agencies, but I think it's important to keep in mind the volume of commerce that's taking place over the Internet when thinking about these numbers. Let me give you some numbers about eBay.

Every single day on eBay there are over 6 million items put up for—that are on sale by people all over the world. Every day over 1 million items right now are being added for sale on eBay. Over 2 million bids every single day are being placed for items from users, and we have, according to our last report, over 29 million users. We have websites in 19 countries, and we have users in virtually every country in the world. For every second, on every second on eBay, $251 in business is being transacted. That's $251 per second, 24 hours a day, 7 days a week. If you took our numbers from the first quarter this year, assuming no growth, that's $8 billion worth of gross merchandise sales for 2001.

Looking at some of the complaints, Federal Trade Commission in 1999——

Mr. SMITH. Why haven't you offered members stock options? [Laughter.]

Mr. CHESNUT. I'm trying to get some myself.

You know, if you look at some of the numbers—because the growth is really phenomenal. In 1999 we ran 125 million auctions on our website, and during 1999, that same period, the Federal Trade Commission received 14,000 complaints about—relating to online auction fraud, and that's industry wide. In the year 2000 the number of listings on eBay more than doubled from 125 million to 260 million. You would expect that the number of complaints to the Federal Trade Commission would have increased by more than double as the business grew by more than double. In fact, the numbers went down as an absolute number, to 11,000. Why are the number of auction fraud complaints going down with the FTC? I think it's been a combination of a number of things. I think law enforcement is catching up, the training, their efforts in these cases. They're to be commended. I think that the Government has also done a great job of educating people about how to trade smart online. I also think that we've been able to do some things that have been successful, and let me just mention a couple.

One, say payments. You know, when we originally came online most of our users were doing business with money orders, sending

checks, cashier's checks to other individuals, and that's a process, a payment process that offers no recourse if you send the money and you don't get the goods. And what we've been able to pioneer is a payment method where consumers can pay each other through credit cards, where ordinary consumers, like you and I selling things to each other out of our garage, can pay each through credit cards using a third-party bank, a service. eBay, I know is in partnership with Wells Fargo Bank and Billpoint through one of those services. So if there is a problem and if the item doesn't arrive, or if the item isn't as advertised, the consumer's got full recourse, 100 percent protection through the charge-back protections of their credit card. And I think that's the wave of the future really in dealing with online person-to-person trading fraud, as it's been reported.

On top of that, we also offer third-party escrow, so that if a consumer wants to send the money to a third party and have that third party hold onto the money until the goods arrive, they've got that available.

On top of that, we have made a business decision that we're going to insure transactions on our website, every single one of them, up to $200. Cost of doing business. People don't have to pay for that insurance. It's automatic. So if a consumer has a bad experience on eBay, doesn't get the goods as promised, we're going to protect that up to $200 with a $25 deductible.

We've also had a lot of success with an education program, we're actually working with the Government to teach people about what they can and can't do online. The best example is something we've done with the Consumer Product Safety Commission. We've given the Consumer Product Safety Commission free web space on eBay, as well as a number of other Government agencies like the U.S. Customs Service, where they can teach consumers on eBay about their mission, and consumers can actually learn about safe trading directly from the Government. I know that in the month after we partnered with the Consumer Product Safety Commission, hits on their database tripled. They had to go out and buy new servers because we were able to drive so much traffic to them from consumers who really wanted to learn more about how to trade safely and make sure they didn't buy recalled products.

The last thing I'm going to mention is our Fraud Investigation Team. My wife used to be a special agent with the INS before she came to eBay. She now manages a full-time force within eBay that does nothing but work with law enforcement every day, full time. And we have contacts, literally thousands of contacts in law enforcement, not just in the United States, but worldwide, so that if a consumer has a problem on eBay, they need to get in touch with law enforcement. My wife's team works with them, gets cases promptly to the right person in law enforcement so that we can prevent further losses and get the cases investigated.

A number of other efforts we have are detailed in my statement, but I'll finish here.

[The prepared statement of Mr. Chesnut follows:]

PREPARED STATEMENT OF ROBERT CHESNUT

Mr. Chairman and members of the Subcommittee:

My name is Robert Chesnut, Vice President and Deputy General Counsel of eBay, Inc. ("eBay"). eBay is the world's first and largest online trading community. It was founded in September 1995 and currently has over 29 million registered users. Essentially, eBay's business is to bring together buyers and sellers from across the United States, and the world, to facilitate trading of goods and services.

I appreciate the opportunity to testify today about some of the creative steps being taken by private industry to fight crime online and the cooperative approach that we at eBay have found with federal and state law enforcement officials. Finally, I will conclude my testimony with a brief discussion of one problem that eBay believes needs new federal legislation—a criminal prohibition against email address harvesting for the purpose of sending illegal spam. Such a prohibition, will eliminate another area of cybercrime and make the Internet safer.

EBAY'S EFFORTS TO ELIMINATE ONLINE CRIME

When I first came to eBay two and one-half years ago, I heard many people marvel at what a tough task it must be to fight crime on the Internet, and how the Internet presented so many challenges to lawful business activity. But what I have come away with from my work at eBay is that the Internet provides law enforcement and private businesses so many opportunities to fight crime with creative solutions, many of which could exist only because of the Internet. Let me highlight some of the creative measures we use at eBay that have had a significant impact in combating unlawful activity on our website.

1. Our *"Feedback Forum"* gives users the opportunity to share their experiences with other users—every user of our service has a numerical feedback profile available for all to see so that good sellers and buyers are rewarded for fair dealing and bad ones are weeded out for failing to do the right thing.
2. Our *Verified Rights Owners' Program* (VeRO) protects intellectual property owners—it is a highly successful joint effort between eBay and private rightsowners (more than 2,000) as diverse as Adobe, the MPAA, Muhammad Ali and Bruce Springsteen to identify pirated goods, take them off our site and report repeat infringers to law enforcement.
3. Our *education program* teaches users about the law, and explains in plain English why certain items (like prescription drugs, alcohol and tobacco, items made from endangered species) cannot be sold on eBay. This is a permanent part of our site devoted solely to the law, and we have built it by creating partnerships with state and federal agencies. We provide free web space to government agencies right on our site to teach users about key laws that might affect their ability to trade, and many agencies, including the Customs Service, the Environmental Protection Agency (EPA) and the Food and Drug Administration (FDA) are using our services.

   For example: in early 2000, eBay approached the Consumer Product Safety Commission (CPSC) and proposed a joint project to prevent users from trading recalled goods on the Internet. Within weeks, the CPSC had a free web page within the eBay site that linked to the CPSC records on recalled products, and users in key categories like baby items, power tools and sporting goods were encouraged to check out their items on the CPSC website before buying or listing them for sale on eBay.

   The result? Amazing—In the first month, queries to the CPSC recall database tripled, requiring the agency to add new servers to handle the loadYand many consumers were educated about recalled products, a positive outcome for the agency and eBay users.
4. We have made large strides in improving methods of safe payment for goods and services traded on our site. We encourage and support third-party escrow services that allow buyers to send money to the service receive the goods from the seller and then release the funds to the seller. Escrow protects both parties to the transaction. We have partnered with Wells Fargo Bank in a service known as *Billpoint*. Billpoint allows users to pay for items with a credit card, even when the are buying items from ordinary people who are not merchants and that could otherwise not accept credit card payments. This brings the protection of credit cards into person-to-person trading on the Internet. Consumers who pay with a credit card have nearly complete protection against fraud through charge back rights provided by credit card issuers. Billpoint has already paid significant dividends in the fight to protect consumers on the Internet.

5. And when things do go wrong (and unfortunately they will go wrong whenever ordinary people do business directly with each other from remote points around the globe), we have devised additional new strategies to assist them. One important element is online mediation. eBay played a key role in the formation of the *online mediation* industry and its leader Square Trade. Square Trade helps consumers resolve disputes with each other (even in different language from all over the world) with the help of professional mediators online. This program is subsidized by eBay so that users never have to pay more than $15 to have a case mediated online. The response has been overwhelmingly positive. It is cost efficient even for small disputes between users anywhere, the legal system is not clogged with these small matters, and users love an independent voice of reason that is often crucial to resolving online disputes. Square Trade handled over 60,000 disputes in 2000 and nearly 90% were concluded with positive results for both parties.
6. Similar to the offline world, we have witnessed larger fraud cases involving a number of victims. eBay has attacked the problem with the creation of our *Fraud Assistance Team*. The Team devotes themselves full-time to putting victims in touch with the right law enforcement agency who can help them, from Hong Kong to London to New York and California. We work with law enforcement to get them key records in a matter of hours, not days. We have created electronic victim's complaint forms that can be filled out online and emailed directly to an investigative agent in a matter of hours. This is crucial to gathering evidence from many victims around the globe. Law enforcement is so impressed with the tools we place at their disposal that in the last month, one federal prosecutor in Illinois stated that eBay's cooperation was Aphenomenal.@ The best he had ever seen from a private company. Another federal prosecutor in Alabama told us last week that without our work in putting a case together, the case would have never been prosecuted. Most importantly, cases are getting prosecutedYdozens of Internet criminals are going to jail, paying fines and returning money to victims in state and federal cases across the country and around the world. Each successful prosecution sends an important message that the law does apply on the Internet and particularly on eBay.
7. And when all else fails, eBay provides a *free insurance* to *all* its users through Lloyd's of London—if a transaction goes bad, eBay makes good on it, up to $200. It is automatic—no premiums or pre-registration. For eBay, it is a cost of doing business and takes a lot of the sting out of bad experiences. How many bad experiences occur on eBay? Less than $^{1}/_{100}$th of 1 percent of all listings on eBay result in an insurance claim payment,. a record we would match with any other retailer anywhere in the world any day of the week.

THE RESULTS

Are these creative strategies working? The latest statistics suggest that these strategies are making a significant difference. In 1999, the FTC received 13,091 complaints about online auction fraud. Remember that not all of these complaints are actual fraud . . . many of these complaints were resolved by the users after the complaint was filed, or were never fraud in the first place . . . and not all involved eBay. During 1999, eBay alone hosted 125 million listings of goods and services.

In 2000, eBay grew at a dramatic pace, hosting more than twice as many listings—approximately 265 million. But the number of FTC fraud complaints? They went down, to 10,872 . . . a remarkable drop, almost 20%, particularly when compared with the growth of the industry. We are proud of these numbers, and we are committed to introducing new measures to continue these positive trends in 2001 and beyond.

THE NEED FOR ANTI-HARVESTING LEGISLATION

It is worth noting that some forms of cybercrime could be reduced if Congress were to adopt a criminal prohibition against the automate harvesting of email address for the purpose of sending illegal Spam. eBay users are increasingly receiving illegal Spam, from people who obtained their email addresses illegitimately from the eBay web site. These harvesters are building a growing and lucrative business by attacking popular websites with automated tools that suck in millions of e-mail addresses and spew them out again for use by Spammers. This parasitic process undermines public confidence in e-commerce, feeds public fears about threats to privacy on the Internet and becomes a breeding ground for fraudulent conduct.

All of eBay's anti-fraud activities, outlined above, are undermined when Spammers convince eBay users to engage in transactions off the eBay site. We believe that a cybercrime bill should include a provision, amending the Computer Fraud and Abuse Act, 18 U.S.C. Section 1030, to outlaw the automated bulk harvesting of e-mail addresses for the purpose of sending illegal spam. Such a provision will guarantee additional protection to America's online consumers.

Thank you. I am available to answer any questions you may have.

Mr. SMITH. Thank you, Mr. Chesnut.

And that's the second reference, Mr. Harris, to immigration so far. I might say that I know a number of other people, and that includes myself, are relieved that I was able to become Chairman of the Crime Subcommittee, but I appreciate what your wife is doing for the INS.

Mr. Kruger.

STATEMENT OF ROBERT KRUGER, VICE PRESIDENT FOR ENFORCEMENT, BUSINESS SOFTWARE ALLIANCE

Mr. KRUGER. Mr. Chairman, no references to immigration in my testimony.

Good morning. My name is Bob Kruger. For the past 8 years I have been Vice President of Enforcement at the Business Software Alliance, an association of leading software and e-commerce developers. Prior to that I was a Federal prosecutor.

While we sit here this morning, perfect copies of software programs that cost American businesses hundreds of millions of dollars to develop, are being unlawfully copied, counterfeited, sold and downloaded from the Internet. Those acts are costing the economy billions of dollars in lost sales and millions of lost jobs every year.

Digital piracy is not a new phenomenon for software publishers. It has always been possible to make perfect copies of software programs, but it is a problem that is now worsening. The card table pirate, who used to sell to dozens of customers at flea markets, now reaches millions through Internet auction sites and e-mail spams. Counterfeiters, including organized criminal groups, have discovered that if you don't have to pay anyone for the research and development of those programs, selling them is a high-margin and low-risk proposition.

And a new species of pirate has emerged, one who sets up sites on the Internet where software can be freely downloaded, inviting the world to loot some of the crown jewels of the American economy. Software developers also face a problem on the demand side as new generations of computer users come to believe that because piracy is so rampant it can't be so bad. If it was, they reason, someone would do something about it.

For its part, the industry is working very hard to combat piracy. BSA's members are pouring resources into this effort, diverting money and manpower that would otherwise be used to develop new products. We are pursuing education and awareness campaigns. For example, BSA recently obtained a DOJ grant to develop educational programs to prevent intellectual property theft and cyber crime. This effort will include creating public service announcements that reach out to American youth with the message that piracy is wrong. We are seeking to forge partnerships with and enlist the cooperation of Internet businesses. BSA has, for example, issued a set of model business practices for Internet auction sites,

designed to reduce the incidence of piracy. We are making ample use of the notice and takedown procedures set out in the Digital Millennium Copyright Act, and we are aggressively pursuing civil litigation against auction vendors and other types of Internet pirates.

But in addition to these industry efforts, there is a critical need for Federal law enforcement attention to this problem. Thanks to congressional action, tools needed for effective prosecution already exist. I commend Members of this Committee for passage of the No Electronic Theft Act, and for your leadership in securing enhancements to the Federal Sentencing Guidelines for intellectual property crime.

There are several reasons why Federal prosecutions are an important part of the solution to this problem. First, we are in a period of tremendous opportunity. Attitudes and behaviors are still forming over the issue of respect for intellectual property online. Effective action to close the barn door now will have greater impact than years of chasing the horse later one. Second, criminal prosecution and penalties provide deterrence in a way that civil judgments cannot. Pirates need to know that they stand to lose not just money, but also their liberty. Third, law enforcement has investigative capabilities unavailable to private industry, such as subpoena and search warrant authority, and the ability to enlist the assistance of law enforcement agencies overseas. And finally, because of the preemptive effect of Federal copyright law, State and local enforcement agencies are limited in what they can do. In effect, Federal prosecutions are the only game in town.

Now, we have seen some signs of progress. There have been an increase in the number of software piracy prosecutions announced by the Justice Department this year. Last month a Federal jury in Chicago returned a guilty verdict against a member of the Pirates with Attitude software ring, after the first trial under the NET Act. The jury's verdict, reached in a mere 30 minutes, is a statement that the public, like Congress, condemns software piracy. We also applaud recent efforts by the Customs Service to fight counterfeiting, particularly by international organized rings, and we welcome the Attorney General's statement before the full Judiciary Committee that fighting piracy will be a priority within his department.

But to be effective, the law enforcement effort requires sustained activity. Resources must be adequate. Agents and prosecutors must be well trained. Cases must be aggressively pursued, and attention must be paid to communicating the deterrence message as broadly as possible.

Mr. Chairman, we look to this Committee to ensure that law enforcement remains a integral part of the solution to this problem. We ask that you continue your oversight to preserve the positive momentum that has been building. BSA stands ready to assist you in any way to address these important issues.

[The prepared statement of Mr. Kruger follows:]

PREPARED STATEMENT OF ROBERT KRUGER

Good morning, my name is Bob Kruger. I am Vice-President for Enforcement for the Business Software Alliance, an association of leading software and e-commerce

companies.[1] I thank the Committee for the opportunity to testify about a matter of great concern to the software industry. BSA's members create approximately 90% of the office productivity software in use in the U.S. and around the world. I would like to give the Subcommittee some background on the state of software piracy today, what the industry is doing to protect itself and the critical role that law enforcement must play. Congressional attention to the piracy problem has been invaluable in meeting the serious challenges faced by copyright owners in the past and will be needed to ensure that creators of IP can continue to make important contributions to the economy in the future.

MY BACKGROUND

I have been BSA's Vice-President for Enforcement for eight years. Prior to my joining the Business Software Alliance, I served as a federal prosecutor in the U.S. Attorney's Office in the District of Columbia and before that as Associate Counsel to President Reagan. During my tenure at the Business Software Alliance, I have learned firsthand how pervasive, multi-faceted, and resistant the software piracy problem is and what a devastating impact it has on software developers.

THE PROBLEM

BSA was formed by leading software companies to combat a major threat to their markets, domestic and overseas, and to their ability to continue to create new programs. That threat is piracy. Software publishers occupy something of unique position when it comes to digital piracy. It has always been possible to reproduce and distribute perfect copies of software programs because from its creation software is available only in digital form.

A look at software piracy statistics provides insight into the scope and severity of the problem. Every year the International Planning and Research Corporation undertakes an international survey of the level of software piracy on a country-by-country basis along with its economic impact. Last month, BSA released the survey for the year 2000. On a worldwide basis, the survey found that the piracy rate averaged 37% resulting in revenue losses of $11.75 billion dollars. In a few countries, the piracy rate exceeded 90%. In the US, the piracy rate for 2000 was 24% with a revenue loss of $2.6 billion. These numbers are very high, but they actually represent an improvement from the 1994 statistics when the international piracy rate was 49%—meaning that half of the world's software was pirated. Unfortunately, after several years of decreasing software piracy rates worldwide since 1994, we've witnessed a slight increase from 1999 to 2000. Several factors were responsible for this increase, notably the growth in the total software market in developing nations where the software piracy rate far exceeds the world average. The market growth in these nations was not offset enough by market growth in more established nations with lower piracy rates.

The statistics collected in this study reflect the real financial harm piracy inflicts on American software companies. Publishers invest hundreds of millions of dollars every year and immeasurable amounts of creativity in designing, encoding and bringing new products to market. They depend upon the revenue they receive from those products to obtain a return on their investment and to fund the development of new products. The impact of software piracy extends beyond the lost sales. Piracy results in thousands of lost jobs and millions of dollars in lost wages and tax revenue.

For years, software piracy has generally been practiced on a limited, if not small, scale. Its scope and its reach were constrained by such factors as time, physical space, geography and production and distribution costs. It is now possible to see that period in time as "the good old days." Four trends explain this change:

- The online market is exponentially larger than traditional retail markets for pirated products.
- Technology can result in the creation of better software tool for consumers; misuse of that technology also makes the theft of intellectual property much easier and faster to accomplish

[1] Since 1988, the Business Software Alliance has been the voice of the world's leading software developers before governments and with consumers in the international marketplace. Its members represent the fastest growing industry in the world. BSA educates computer users on software copyrights; advocates public policy that fosters innovation and expands trade opportunities; and fights software piracy. BSA members include Adobe, Apple Computer, Autodesk, Bentley Systems, CNC Software/Mastercam, Compaq, Dell, Entrust, IBM, Intel, Intuit, Macromedia, Microsoft, Network Associates, Novell, Sybase, and Symantec. BSA websibes: www.bsa.org; www.nopiracy.com.

- It's harder to catch and take action against perpetrators who operate on the Internet
- Software theft has become an attractive enterprise for organized crime

First, the Internet has exponentially expanded the market for pirated software. Contrast, the number of people who can crowd around a card table at a flea market with the number that can simultaneously access and download software from a pirate website. Instead of pirated copies being sold one at a time, millions of pirated copies can be downloaded every day. Geography no longer matters. A pirate can sell and transfer stolen intellectual property to someone located here in Washington, DC, just as easily as he or she can sell and transfer it to someone in Australia.

Second, the Internet has also made locating and obtaining pirated software much easier. Consumers in every city can use the phone book to find legitimate software vendors who have a real, physical location. There is, however, no phone book or other tool to locate software pirates who operate from real, physical locations. But computer users can easily employ an Internet search engine to find both legitimate and illegitimate sellers of software. Or consumers can visit popular auction sites and what appear to be legitimate websites to find pirated or counterfeit products that often purport to be genuine. From the buyer's perspective, the Internet also significantly lowers the stigma of knowingly purchasing stolen goods by allowing the transaction to occur in the comfort of one's house or workplace. Advances in bandwidth and compression technology enable downloading to occur in a fraction of the time previously required.

Third, the ability of Internet pirates to hide their identities on the Internet or operate from remote jurisdictions makes it that much more difficult for rights holders to take responsive action or hold them accountable. Once BSA's investigators identify where pirated software being distributed online, they can have a much harder time finding the responsible party than in the offline world. We do not have, nor would we want, surveillance capability and our ability to establish the true identity of website owners, spammers, vendors can be limited by their efforts to avoid detection and legitimate privacy concerns. Intellectual property owners can and do use online tools. For example, the Whois database lists the registered owner of a website, although the information is sometimes false or out of date. False Whois contact information may be an issue that this Committee wishes to look into further.

Let me give you an example of how complicated an Internet investigation can be—a software pirate who lives in Canada can advertise his stolen products on a website hosted by a Chilean Internet Service Provider that lists an email address in India as the point of contact. After an email from the seller directing the purchaser to wire money to a bank account in Japan, the pirate then tells the purchaser via an anonymous email account to go to a website in Mexico to download the software. In order to build a successful case, BSA must work with authorities in each of the countries even though none of the illegal activity occurred in the pirates's home country of Canada. Obviously, this complicated scenario is fortunately uncommon, but it does show the complexity of what we can and do face on a daily basis.

Finally, the presence of very large amounts of high quality counterfeit software in the market continues to pose a serious problem for BSA's members. During the past 12–18 months, we have seen a dramatic increase in the amount of high quality counterfeit software imported into the U.S. from overseas, especially from Asia. Moreover, international counterfeiting rings have become even more sophisticated in their methods of producing "look alike" software and components. For example, recent raids in Hong Kong uncovered evidence of sophisticated research and development laboratories where counterfeiters reverse-engineered the security features of at least one member company's software media. Not surprisingly, investigations in Asia, Europe, and Latin America have revealed the involvement of serious criminal organizations in the manufacture and distribution of high quality counterfeit software. Compared to loan sharking, bank robbery, and protection rackets, software piracy is an easy, rarely prosecuted crime. Finally, the Internet has transformed the business of distributing counterfeit software, making possible for major exporters in Asia and elsewhere to sell directly to corrupt resellers anywhere in the world. One recent example demonstrates the potential of this distribution method to cause serious harm to U.S. software publishers: during a period of only three months, a small reseller operating out of trailer in Flugerville, Texas, imported over 47,000 counterfeit copies of Microsoft® Office and Windows® programs, with an estimated value of $13 million.

HOW DOES SOFTWARE THEFT OCCUR ON THE INTERNET?

There are two primary means of software theft that occurs on the Internet: retail piracy and downloading. Retail piracy includes of auction and mail order websites along with email spam advertising pirated programs. Basically, the card table vendors have migrated online. As I noted earlier in my testimony, they can reach an international marketplace 24x7. By making their wares available on legitimate commercial sites such as auction sites, pirates acquire a patina of legitimacy.

Downloading theft occurs on a wide range of sites and locations where users can download unauthorized copies of copyrighted software programs, e.g, web sites, IRC channels, newsgroups, and peer-to-peer systems like Gnutella. The persons who are making these programs available are essentially throwing a brick through the storefront window and inviting others around the world to loot at their leisure. Clearly, this conduct is not tolerated in the bricks and mortar world and it should not be tolerated online.

WHAT THE INDUSTRY IS DOING TO PROTECT ITSELF

The members of the Business Software Alliance are in the business of developing popular software programs, not enforcing their intellectual property rights. I know for a fact that they would rather spend the money they pay me to hire another programmer. It is, therefore, a testament to the impact piracy is having on their businesses that they devote considerable financial and human resources to copyright education and awareness campaigns, policy initiatives, and enforcement actions.

The Business Software Alliance does not solely take a reactive response to software piracy. Indeed, BSA's worldwide piracy campaigns emphasize education, awareness and compliance over enforcement. Our website offers tools for end-users to determine if their installed software base contains an appropriate number of licenses. Other public awareness projects are also listed on our website. Even our enforcement efforts are undertaken with an eye towards sending the message as widely as possible that it is more expensive to violate copyright laws than to comply with them in the first place.

As an example, let me describe just some of what BSA and its members are doing to protect themselves against piracy in its modern form:

- Notice and takedown programs: BSA maintains a team of investigators in the U.S. and in Europe with additional coverage in Latin America and Asia. We constantly receive referrals from our members, complaints from consumers, and identify infringing activity through proactive investigation. Thousands of notices to ISPs, auction sites, redirect services and others have been sent this year alone. In the United States BSA and other intellectual property owners use the Digital Millennium Copyright Act (DMCA) passed in 1998 to shut down US based websites that contain stolen software.
- Civil litigation: BSA's members have filed suit against dozens of individuals offering pirated software for free download on an Internet relay chat channel that caters to cable-modem users. In November, BSA filed suit against thirteen vendors who offered pirated software for sale on popular Internet auction sites. To give you some idea of how brazen some of these software pirates can be, at least four of those thirteen vendors continue to sell pirated software even after being sued.
- Model business practices for auction sites and ISPs: Software publishers seek the cooperation and engagement of other Internet entities in protecting intellectual property and reducing the incidence of piracy. BSA has, for example, developed model business practices for Internet service providers and for auction sites. We have already received the public support of Amazon.com for the auction site practices and are working with other sites to gain their support.
- Companies are exploring technological solutions that balance interest in intellectual property protection and legitimate needs of users. Experience indicates, however, that there is no silver bullet technological solution to what is, at bottom, an ethical problem.

THE NEED FOR FEDERAL LAW ENFORCEMENT OF U.S. COPYRIGHT LAW

Notwithstanding all of BSA efforts in this area, there is a critical need for engagement by federal law enforcement authorities in combating this problem. And thanks to Congressional attention, the tools needed for effective investigation and prosecutions already exist. I commend the members of this Committee for passage of the No Electronic Theft (NET) Act in 1998 and for its leadership in securing enhancements to the federal sentencing guidelines for intellectual property crime.

There are several reasons why federal law enforcement is a critical component of an effective approach to combating piracy:

- We are now in a period of tremendous opportunity. Attitudes and behaviors are still forming over respect for intellectual property online. Congress has spoken in the form of strong laws against piracy, but Congress' voice can only be heard if law enforcement plays its role and prosecutes those laws.
- Only criminal prosecution and penalties can provide effective deterrence. The threat of a civil judgment is insufficient to deter pirates, many of whom already operate on the margins of society. Pirates need to understand that breaking the law could force them to surrender something more precious-their liberty.
- Law enforcement brings superior investigative capabilities that private industry does not have access to such as search warrants.

Software publishers are used to operating in Internet time in which taking years to ramp up or respond can be fatal to a company's bottom line. That is why we have been frustrated in the past by the length of time it has taken to see some meaningful progress in the number of intellectual property cases prosecuted. We are encouraged though by recent indications that intellectual property cases are receiving a higher priority. Ten software piracy cases have been reported on the Department of Justice Computer Crimes and Intellectual Property Section's website this year. While hardly a torrent of activity, that number compares quite favorably to the two such cases announced last year and the one in 1999.

Prosecutions under the NET Act are one indicator of DOJ's willingness to combat Internet piracy. We are encouraged, therefore, by the fact that just last month, the U.S. Attorney's Office in Chicago secured a the first conviction by jury trial of a defendant prosecuted under the NET Act. The defendant was a member of the notorious "Pirates With Attitude" software ring. Although there had been previous pleas under the NET Act, a conviction after trial is the truest validation of whether a new criminal statute operates as intended and can serve as an effective prohibition and deterrent. And while there have been other prosecutions of Internet piracy, nothing demonstrates law enforcement's commitment better than taking a case through trial. Finally, a guilty verdict embodies more than legislative or prosecutorial condemnation of particular conduct—it reflects, in the purest sense, a popular judgment that Internet piracy is and should be a criminal offense. In short, the people have now spoken. For pirates out there who were hoping that they would be let off the hook by a jury of their peers, this has to be a major disappointment. To underscore the jury's feelings of the strong case against the defendant, I would point out that the jury deliberated for only 30 minutes before rendering their guilty verdict.

BSA also applauds the recent efforts by federal law enforcement agencies, particularly the U.S. Customs Service, to devote more resources to fighting counterfeiting. We are aware of international investigations currently being pursued by Customs and several U.S. Attorneys involving the importation of hundreds of thousands of counterfeit CDs. The aggressive pursuit of the organized criminal rings involved in these cases stands out, and is extremely important to our members. At the same time, however, the overall federal law enforcement resources devoted to anti-counterfeiting efforts is still quite inadequate. We are aware of more than a few cases where raids have been delayed or not pursued at all because of the lack of prosecutorial or agent resources. In addition, lack of prosecutorial interest in pursuing these cases continues to pose a serious obstacle to effective enforcement in some jurisdictions.

There is still work to be done in new areas of software theft. Coordinated action against mail order piracy is necessary to end the consumer fraud and the crime against the rights holder that occurs when an auction site is used to sell pirated or counterfeit software to sometimes unsuspecting buyers. We also need assistance in engaging law enforcement overseas.

OTHER ACTIONS THE FEDERAL GOVERNMENT CAN TAKE TO FIGHT SOFTWARE PIRACY

The message also needs to be sent to our nation's youth that stealing something on the Internet is no different than walking into a department store and stealing a sweater or videocassette. To that end, the Hamilton Fish Institute on School and Community Violence at George Washington University and BSA recently obtained a grant from the Department of Justice for the "Crime Prevention and Educational Programs for Intellectual Property Theft and Cyber Crime" project. This project will better define the scope and nature of electronic crime and will identify effective education strategies to raise public awareness about cyber crime. Part of this effort will

be to create public service announcements that reach out to American youth with the message that piracy is wrong.

THE ROLE OF CONGRESS

Your continued oversight of DOJ is necessary to ensure that software piracy prosecutions are a serious threat and therefore deterrent to those who would plunder the results of someone else's hardwork, investment and creativity. Last week, Attorney General Ashcroft testified before the full Judiciary Committee that

> "I can say to you that we take very seriously piracy and theft and the invasion of privacy and a whole variety of issues that are related to the advent of the capacity of individuals to utilize the computer both in the industry and personally. And given the fact that much of America's strength and the world economy is a result of our being the developer and promoter of most of the valuable software, we cannot allow the assets that are held electronically to be pirated or infringed, and so we will make cyber crime issues a priority and additional resources have been requested in next year's budget for that and that's not just in this Administration's submission regards to the FBI budget"

Actions that back up statements like this are the only way that software pirates can be stopped either directly by cases brought against them or by receiving the message that software theft is not an easy crime. In FY2000 Congress approved dedicated appropriations for fighting cybercrime. Continued efforts such as this will ensure that DOJ investigators and prosecutors will have the necessary resources to bring these cases.

CONCLUSION

I would like to thank the Subcommittee again for the opportunity to testify today. Only through a combined effort of by intellectual property owners, educators, policymakers and the law enforcement community will the scourge of software piracy be reduced. I would be happy to answer any questions this Committee may have.

Mr. SMITH. Thank you, Mr. Kruger.
Mr. McCurdy.

STATEMENT OF DAVE McCURDY, PRESIDENT, ELECTRONIC INDUSTRIES ALLIANCE

Mr. MCCURDY. Thank you, Mr. Chairman, and thank you for the opportunity to testify today. I appreciate the invitation, as well as Mr. Scott.

Mr. Chairman, I ask that my testimony be submitted in the record full, because I want to summarize, and I'll leave it to you all to read the testimony, but there are a couple points that I'd like to summarize.

Mr. SMITH. All right. Without objection, the complete testimony of all witnesses will be included in the record.

Mr. MCCURDY. Mr. Chairman, I want to commend my colleagues on the panel today because I think they've stated very clearly the nature of the problem and the significance of it. And I think we're preaching to the choir in the recognition of the problem. This is not a question of "if", it's a question of "when" and "how much."

If I can, refer just to a quick chart. This is a chart, and it's actually, I think, attached, included in the statements for the panel members or for the Committee. These are the number of incidents reported to the CERT Center at Carnegie Mellon. You can see just the pure graphics, that up until 1999, there were less than 5,000 incidents reported. Each incident is a different kind of attack, whether it's a virus—the "I love you" counts as one on this chart. But from 2000, 2001, it jumped over 22,000 reported incidents. So you can see the trend line is very significant. The types of attacks are increasing.

The important thing that goes with that, Mr. Chairman, is as on one hand, the tools that are available today to perpetrate these attacks have increased. We're no longer in the password guessing game. We're using sniffers and scanning techniques. We have sweepers that live on the Net. You now can go into—and I'll give you some examples of these—tremendously collaborative tools that are available to relatively unsophisticated users and attackers, so you no longer have to be a software genius to be able to perpetrate the attacks. So this is a dangerous trend line that is reported here.

There was a recent report, Mr. Chair—and actually, if I could, at some point we'll get this site for you, but this is a marvelous forensic analysis by a person, Steve Gibson, at the Gibson Research Corporation, after they were subjected to a denial-of-service attack. And they had two T-1 lines, a lot of gigabit capability. They were completely shut down. He went to the FBI. Didn't get any help; he didn't meet the threshold. And he went to the ISP, didn't get any help. So he went and worked his own way to try to find an answer, and tracked it down. Come to find out it was a 13-year-old person that was collaborative working with others, using 455 Zombie computers, that you and I may have if we're online all the time. Our computer can be taken over with software, and then used to initiate attacks against third parties. It's a marvelous story. It's long, but it's worth reading.

But when you read that story, you also find that the different types of attacks have changed. From January to June of this year there were new vulnerabilities in software products that were reported from at least 39 different countries. While more traditional models of security often focus on the perimeter defenses, securing your own network from unauthorized access, this model is insufficient for today's networks for a variety of reasons, including the level of technical sophistication and the tools that are now being used.

Some of the attacks that were shown and some of the tools were virus, denial-of-service, reconnaissance, misuse of resources, deception, false alarm, hoaxes. But we now see that 54 percent couldn't identify the real source. And I don't know, I'll leave it to you, much smarter than I, but I think it was Socrates said that the real knowledge is knowing that we don't know, and so I think there's a lot of this that still needs to be investigated and followed through.

And there is no magic bullet, silver bullet to solve this. So it takes more—and this is where Mr. Miller and I agree—this is no longer just an issue of cyber crime or national security, this is an economic security issue that needs to be addressed at the board level and CEO level of corporations working cooperatively to develop policies, best practices, tools, share the information, and working with Government to, when appropriate, to try to address this.

There are a number of policy recommendations. I submit those to the Committee within the written statement, and would be glad to answer any questions with regard to those specifics.

[The prepared statement of Mr. McCurdy follows:]

PREPARED STATEMENT OF DAVE MCCURDY

Chairman Smith, Ranking Member Scott, and members of the Judiciary Subcommittee on Crime: I appreciate the opportunity to testify today on behalf of the Electronic Industries Alliance. I am deeply thankful to the Chairman for holding this series of timely and informative hearings on cybercrime. There are few issues that are of more importance to the 2,300 member companies of EIA than cybercrime and a secure Internet.

This is not news, but it still amazes me how quickly the Internet became such an important part of our lives—both personally and professionally. From the simplest personal task like checking your bank account to the most complicated business transaction, the Internet and information technologies have changed the way we live.

Unfortunately, the Internet was not designed with security, privacy or civil liberties in mind. It was designed to be an open platform for communication, with distributed control and mutual trust among users. I'm sure the architects of the Internet had no concept of what it would become, just as we have no concept of what it will become twenty years from now.

Our dependence on this new technology in all areas of our lives has created a true challenge for policymakers: how to protect users of the Internet from the abusers.

As policymakers contemplate how to best protect the Internet from cybercriminals and try to ascertain the proper role of government on the Internet, the reality remains: as a rule, technology has exponentially outpaced the establishment of sound policy.

Dependence on information technologies has opened the door to a host of vulnerabilities. Cybercriminals take advantage of these vulnerabilities every day, including threats to staff, physical assets, networks, transmission and stored data. Any of these critical parts of our information infrastructure are susceptible to sophisticated attacks from anonymous cyber-operators such as "benevolent hackers", delinquents, industrial competitors, organized crime, foreign adversaries and terrorists.

The question is not whether or not an attack will come—because it will come. The question is what will government and business do to prepare for the next imminent attack and preserve critical systems and assets to maintain operability in the information world.

SOPHISTICATION OF CYBERATTACKS

"Nothing more than a whim of a 13-year old hacker is required to knock any user, site or server right off the internet"—Steve Gibson, Gibson Research Corporation, June 2, 2001

Between January 1, 2001, and June 12, 2001 new vulnerabilities in software products were reported from at least 39 different countries. Furthermore, traditional models of security often focus on perimeter defenses—securing your own network from unauthorized access. This model is insufficient for today's networks for a variety of reasons including the level of technical of sophistication and the tools criminals use to launch attacks has evolved very rapidly. This is further complicated by the ability of intruders to evade law enforcement by launching their attacks from intermediate machines they have previously compromised. Here are some examples of some of the common tools associated with cybercrime activities:

- Automated scanners—programs that scan a range of Internet addresses looking for computers of a particular type.
- Probes—programs that examine a computer, once it is located, searching for one or more vulnerabilities. These vulnerabilities are often present in operating system, network, or applications software. They are problems because even when corrected by vendors, system owners often do not upgrade their software with those corrections.
- Root kit—a program that takes control of a penetrated computer and disguises its presence so the legitimate system owners don't know that the system has been compromised. Once a computer is compromised in this way, the attackers have full access to all data on that computer and often to all data on the local network the computer is connected to.
- Sniffers—programs that are installed on compromised machines to scan network traffic as it passes by and look for data the attackers can use to their advantage (computer account names and passwords, credit card numbers, and other unencrypted sensitive data).

- Attack networks—compromised computers that attackers aggregate into networks controlled by one or more master computers. These networks can be programmed to attack other machines on the Internet, often with crippling denial-of-service attacks.
- IP spoofing—a technique attackers use to hide the identity of their attack computers and fool (spoof) the attacked machine into believing the attacks have come from a different source.

As the Internet grows,, so does the risk. For the first time, intruders are developing techniques to harness the power of hundreds of thousands of vulnerable systems on the Internet. Using what are called distributed-system attack tools, intruders can involve a large number of sites simultaneously, focusing all of them to attack one or more victim hosts or networks. The sophisticated developers of intruder programs package their tools into user-friendly forms and make them widely available. As a result, even unsophisticated users can use them. Subsequently, serious attackers have a pool of technology they can use and mature to launch damaging attacks and to effectively disguise the source of their activities (See attachments).

Attack technology is developing in an open source environment and is evolving rapidly. Technology experts and users are improving their ability to react to emerging problems, but we are behind. Significant damage to our systems and infrastructure can occur before effective defenses can be implemented. As long as our strategies are reactionary, this trend will worsen.

Current Cybercrime Policy

The control of U.S. cybercrime policy has traditionally been viewed as an issue for the law enforcement and national defense communities—not an economic policy issue. Solutions for cybercrime have been expressed in terms of criminal sanctions, counter-terrorism efforts and law enforcement training rather than the prevention managed by the users of the information assets, like businesses and individuals.

However, law enforcement and national security communities do not have all the answers. In addition to leadership from private industry, the following goals need to be met in any national policy on cybercrime:

- A National strategy from the President after consultation with leadership of constituencies for coordinated responses to threats and attacks, such as was developed for Y2K including:

  Establishment of empowered organizations for sharing information about cyber-threats, attacks and remedies such as the Internet Security Alliance, the sectoral ISACs, and similar government and international groups
- Incentives for industrial and government institutions to adopt top-down policies of institutional security—including information technology/network security—that include:

  Clear designation of responsibility/delegation from CEO

  Creation of risk management plan

  Investments in employee enculturation and user education

  Establishment of best practices regarding high value/high risk environments in information technology, for example:

  Establishment of organizational CIO

  Employee education on IT security practices

  Deployment of best practices technologies

  Firewalls

  Antiviral software

  PKI authentication/encryption for e-mail/Internet

  In government, necessary training and funding for these types of programs.

What we need to avoid in establishing a national policy:

New technology-specific criminal statutes that will result in the hobbling of vendor industries and slowing of deployment of leading edge technologies to the mass of internet users.

Where can the private sector help?

In order to protect all Internet consumers, organizations must search for an industry-led, global, cross-sector network focused on providing solutions to the challenges of the Internet Economy. We are at risk, and the business community must

make it a leadership priority. The following are examples of what the private sector should be doing:

Information Sharing

Maintaining an adequate level of security in this dynamic environment is a challenge, especially with new vulnerabilities being discovered daily and attack technology evolving rapidly in an open-source environment. To help organizations stay current with vulnerabilities and emerging threats the private sector must concentrate on providing the following:

- *Vulnerability catalog:* a complete record of past vulnerability reports. New entries would be added to the catalog as they were reported.
- *Technical threat alerts:* in the form of "special communications" provide early warning of newly discovered security threats and are updated as analysis activities uncover additional information. Ranging from alerts on newly discovered packages of malicious code, such as viruses and trojan horses, to in-depth analysis reports of attack methods and tools, these reports would help organizations defend against new threats and associated attack technology.
- *Member information exchange:* augmenting the basic services listed above, an organization would have to develop an automated information sharing mechanism that allows business and individuals to anonymously report vulnerability, threat, and other security information that they are willing to share with other secure channels.
- *Threat analysis reports:* today the great majority of Internet security incidents are conducted by unknown perpetrators who act with unknown motivations to achieve unknown goals. Managing security risks in the long-term will require a better understanding of the perpetrators and the economic, political and social issues that drive them.

Best Practices/Standards

Effective management of information security risks requires that organizations adopt a wide range of security practices. From basic physical security controls that prevent unauthorized access to computing hardware, to user-focused practices on password selection, to highly-detailed system administration practices focused on configuration and vulnerability management, these practices help organizations reduce their vulnerability to attacks from both outsiders and insiders.

- *Practices catalog:* beginning with existing practice collections and standards, and in collaboration with any participating companies an organization must develop a catalog of practices that span the full range of activities that must be addressed when developing an effective risk management program. The catalog will contain high-level descriptions of the required practices and should be made publicly available

Security Tools

While a sizeable commercial marketplace has developed for hardware and software tools that can be used to enhance an organization's security and a variety of tools can now be purchased, comprehensive tool sets are lacking. To fill the gaps, organizations build their own or find and evaluate public domain tools—a time consuming and expensive activity. An organization would have to establish a tools exchange: a restricted access repository where network administrators only can exchange special purpose tools they have created as well as information about, and evaluation of, public domain tools available over the Internet.

Policy Development

While there are many things an organization can do to enhance its security, some issues require broad action. For example, overall security could be improved through increased information sharing between industry and government, but FOIA (Freedom Of Information Act) regulations deter companies from sharing sensitive information with the government. Other issues like privacy and the proposed HIPPA legislation could also affect network security. An organization needs to identify these overarching issues and work with the appropriate industry and government organizations to advocate policy that effectively addresses the issues.

Other Critical Areas

The current state of Internet security is the result of many additional factors, such as the ones listed below. A change in any one of these can change the level of Internet security and survivability.

- Enhanced incident response capabilities—The incident response community has handled most incidents well, but is now being strained beyond its capacity. In the future, we can expect to see multiple broad-based attacks launched at the Internet at the same time. With its limited resources, the response community will fragment, dividing its attention across the problems, thereby slowing progress on each incident.
- The number of directly connected homes, schools, libraries and other venues without trained system administration and security staff is rapidly increasing. These "always-on, rarely-protected" systems allow attackers to continue to add new systems to their arsenal of captured weapons.
- The problem is the fact that the demand for skilled system administrators far exceeds the supply.
- Internet sites have become so interconnected and intruder tools so effective that the security of any site depends, in part, on the security of all other sites on the Internet.
- The difficulty of criminal investigation of cybercrime coupled with the complexity of international law mean that successful apprehension and prosecution of computer criminals is unlikely, and thus little deterrent value is realized.
- As we face the complex and rapidly changing world of the Internet, comprehensive solutions are lacking. There is increased reliance on "silver bullet" solutions, such as firewalls and encryption. The organizations that have applied a "silver bullet" are lulled into a false sense of security and become less vigilant. Solutions must be combined, and the security situation must be constantly monitored as technology changes and new exploitation techniques are discovered.
- There is little evidence of improvement in the security features of most products. developers are not devoting sufficient effort to apply lessons learned about the sources of vulnerabilities. Until their customers demand products that are more secure, the situation is unlikely to change.
- Engineering for ease of use is not being matched by engineering for ease of secure administration. Today's software products, workstations, and personal computers bring the power of the computer to increasing numbers of people who use that power to perform their work more efficiently and effectively. Products are so easy to use that people with little technical knowledge or skill can install and operate them on their desktop computers. Unfortunately, it is difficult to configure and operate many of these products securely. This gap leads to increasing numbers of vulnerable systems.

SUMMARY

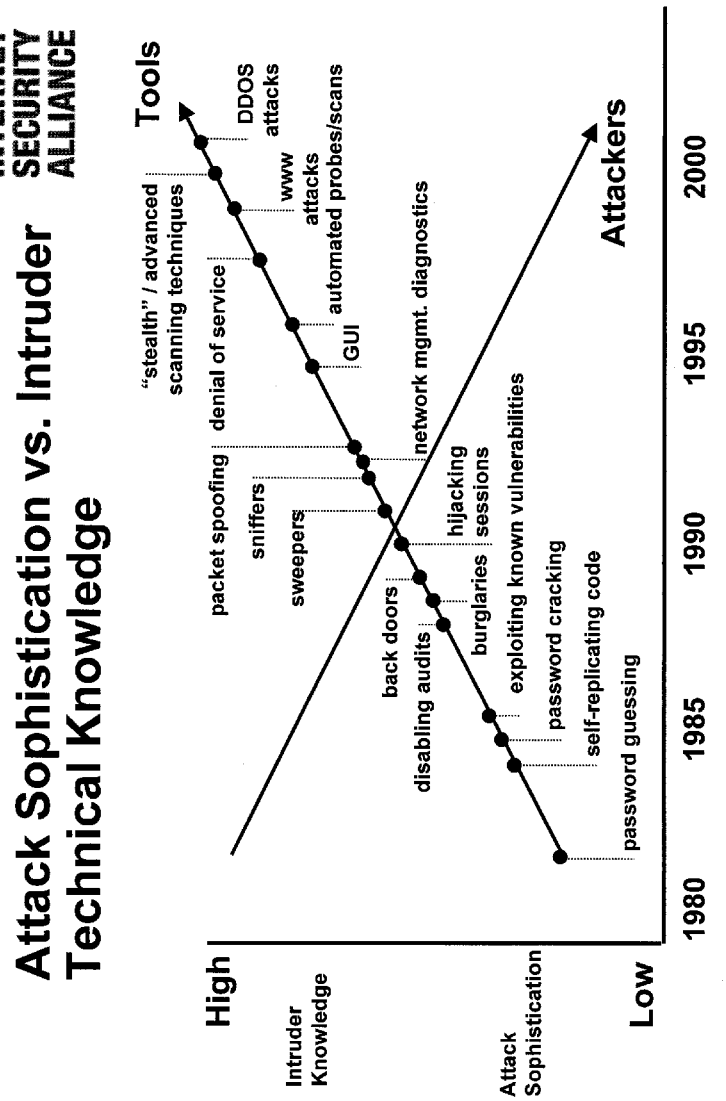
While it is important to react to crisis situations when they occur, it is just as important to recognize that information assurance is a long-term problem. The Internet and other forms of communication systems will continue to grow and interconnect.

- More and more people and organizations will conduct business and become otherwise dependent on these networks.
- More and more of these organizations and individuals will lack the detailed technical knowledge and skill that is required to effectively protect systems today.
- More and more attackers will look for ways to take advantage of the assets of others or to cause disruption and damage for personal or political gain.
- The network and computer technology will evolve and the attack technology will evolve along with it.
- Many information assurance solutions that work today will not work tomorrow.

Managing the risks that come from this expanded use and dependence on information technology requires an evolving strategy that stays abreast of changes in technology, changes in the ways we use the technology, and changes in the way people attack us through our systems and networks. To move forward, we will need

to make improvements to existing capabilities as well as fundamental changes to the way technology is developed, packaged, and used.

Cybercrime needs to be attacked at the security level. Attacks will happen—they will become more sophisticated as our technology becomes more sophisticated. The best defense we can take as a nation is to ensure our networks and systems are properly fortified against attack.



Reports Received by the CERT/CC., SEI at Carnegie Mellon Univeristy

Intrusion Types

Reports	Percentage	Description
733	28.37%	Unknown
701	27.13%	root compromise
419	16.22%	virus
368	14.24%	user compromise
115	4.45%	denial of service
103	3.99%	reconn
76	2.94%	misuse of resources
36	1.39%	deception
17	0.66%	unknown
12	0.46%	false alarm
4	0.15%	hoax
2584		

Domain of Hosts Involved

Hosts	Percentage	Description
161309	5.55%	Government host (.gov)
20328	0.70%	US military (.mil)
2723100	93.75%	Other sites
2904737		

Consequence of Activity

Count	Percentage	Description
1421	54.99%	none specified
343	13.27%	altering web site
157	6.08%	attacking other sites
134	5.19%	install trojan horse
100	3.87%	install back door
86	3.33%	altering configuration
77	2.98%	account creation
59	2.28%	sniffer
41	1.59%	altering logs
35	1.35%	anon ftp abuse
25	0.97%	exposing confidential data
25	0.97%	data destruction
17	0.66%	data altering
15	0.58%	software piracy
13	0.50%	irc abuse
10	0.39%	exposing password file
8	0.31%	fraud
5	0.19%	domain hijacking
4	0.15%	illegal use of machine
3	0.12%	life threatening activity
1	0.04%	credit card fraud
1	0.04%	icq abuse
1	0.04%	query cgi-bin
1	0.04%	rootkit
1	0.04%	exposing dns-zone file
1	0.04%	impersonation
2584		

Mr. SMITH. Thank you, Mr. McCurdy.

As you all know, this is our last of three hearings on a very important subject. We're having more hearings on this subject, in fact, than any other that I'm aware of this year. We hope that these hearings will result in some legislation. Much of the legislation is outdated, and we really haven't had as much or any signifi-

cant legislation since probably the mid 1980's, and we all know what's happened in the high-tech field since the mid 1980's.

I really distilled all my questions to ask each one of you to address. And it is this: specifically what type of cyber crime is the greatest threat to your business or to your membership, and what does it cost in dollars, either you or the economy? And second of all, what specific suggestions do you have for legislation that will help reduce cyber crime in America?

I know, Mr. Kruger, in your written testimony you mention that there was some type—some laws that were not being enforced. If you'll go into a little bit more detail on that.

And, Dave McCurdy, I know that you have a feeling that there are some types of a national policy we should not have and some that we should have. If you'll go into a little bit more detail on that as well. But if you can try to address those two questions in about a minute a person, that would be great. Mr. Miller.

Mr. MILLER. Mr. Chairman, as far as the cost, I think the answer is nobody knows. The Computer Security Institute and the Federal Bureau of Investigation do a survey each year, and they come up with a number, but that number is reported crimes. And as Mr. McCurdy pointed out, and I certainly concur, most of these crimes are not reported because companies simply decide the cost of exposing it is simply not worth the candle. And so I think the answer is we really don't know. And certainly the numbers that the FBI/CSI numbers come up with half a billion dollars, three-quarters of a billion dollars, which doesn't sound like a lot given the size of our economy, but our feeling is the number is in fact a lot larger, particularly given the growing sophistication.

In terms of the greatest threat, the greatest threat is to the fundamental operations and infrastructure. Sure it's a headline when some popular website gets defaced, that's inconvenient, but that really isn't a threat to basic electronic commerce. So the focus has to be on when businesses is actually being done or when Government work is actually being done. The surveys that ITAA has done, with EDS for example, show that 65 percent of consumers are unwilling to do electronic commerce because of concerns about security, not privacy, which sometimes people confuse, but the issue of security. So it's a deterrent to people going online and doing commercial activity.

Similarly, a study we did showed that 62 percent of Americans are unwilling to do transactions with Government because of concerns about security, that they are concerned that information that may pass back and forth about whatever the particular transaction they're doing with the Government is at risk, again, not because of privacy concerns, but because of security. So it's a major deterrent.

In terms of specific legislative recommendations, the only one specifically I focused on was FOIA. I think there a couple of issues go beyond. One is the need to deal with this issue internationally. There is an attempt currently underway, that you're aware of, through the Council of Europe, which is kind of an odd-duck organization we know about, to develop some international standards. In theory we support what the Council of Europe is doing, because as we found out last year, for example, with the "I love you" virus,

which was initiated from the Philippines, at the time the Philippines Government had no laws against the crime that was committed, and ultimately they could not prosecute to individuals, even though they were identified. Since then the Philippines has changed the law. So I think what we need to do is to get more international focus to get some standards. The Council of Europe Treaty, unfortunately, is flawed. It's getting better. There have been more dialog. We think some more improvements are needed.

And lastly I would say what Congress needs to do in the Government side of this is to put more money to the effort, and this isn't necessarily your Subcommittee, but what we're hearing is a lot of rhetoric out of the Administration. I think the Administration is committed—and this was also true of the previous Administration, so this isn't a partisan comment—but it comes to really giving the CIOs the financial resources they need to protect the Government infrastructure. The money simply isn't there. If you use as a baseline what the financial services industry uses, which is the most advanced, they spend—about 10 percent of their IT spend goes to security. The Government estimates are around 1 percent, if that. So you simply can't get there from here if you're not going to spend the money, no matter how good the rhetoric is, to put the information technology in place, to train the people, to have good processes, then the security is simply not going to happen.

Mr. SMITH. Thank you, Mr. Miller. Mr. Chesnut.

Mr. CHESNUT. The most important area, I think, is help us protect our websites. You know, eBay, for example, every day we are literally—we literally have people coming at us dozens of times a day at different levels, and we have to spend enormous resources in trying to make sure that these attacks aren't successful and disrupting the operation of our site. If eBay is taken down for any period of time, it not only affects eBay, but we have tens of thousands of people who depend on us to make a living full time. They're selling goods. So if we're taken down, it's not just our business that's being harmed, but their business as well.

So legislation that would help us protect our site by enhancing penalties for people who attempt to hack into websites, denial-of-service attacks. I think that's critical.

In addition, helping us protect our websites against spiders, people who come at us in order to harvest e-mail addresses of our users. You know, we are constantly subjected to individuals who come to our site, steal e-mail addresses, and then use those e-mail addresses to send illegal spam, and often the spam itself encourages illegal activity or is encouraging fraud. And in order for us to really help our users and protect them against fraud, we've got to be able to protect their information and their e-mail addresses against these pirates.

Mr. SMITH. Thank you, Mr. Chesnut. Mr. Kruger.

Mr. KRUGER. Mr. Chairman, the competition for which form of piracy is costing us the most losses is pretty stiff these days. One thing I can say with certainty is that Internet piracy is a growing percentage of the losses that we're suffering. We can't quantify it much more than that, other than to say that we're losing more to Internet piracy tomorrow than we lost yesterday, and that trend will continue.

Credit does go, as I said during my written and my oral testimony, Mr. Chairman, to Members of this Committee for enactment of the NET Act and for the encouragement of the U.S. Sentencing Commission to enhance the Sentencing Guidelines. Those effective tools are out there. They are available. As you said, Mr. Chairman, the question is enforcement using those tools and that's where we think there's much work to be done, and where effective oversight by this Committee in providing law enforcement agencies with the resources they need would accomplish our goal.

Mr. SMITH. Thank you. Mr. McCurdy.

Mr. MCCURDY. Mr. Chairman, just very quickly to your question. With regard to legislation, we do believe that the legislation proposed by Congressman Davis (Va.) on FOIA is a step in the right direction, similar to what occurred with Y2K, because without the information sharing, we're not going to be able to address some of these unknown issues, which is really what the threat is in the long term.

There is a need for a national strategy, and it needs to be led both from the top of Government, from the President on down, but as I said, it needs to be implemented working with the private sector. But there are some things that I think you need to be careful of, and there's always a tendency to look for quick answers and solutions. With a national policy, we should not have any technology specific criminal statutes, because I believe that just ends up hobbling industry and vendor industries, and slowing the deployment of leading edge technologies to the mass of Internet users. And what I'm really saying is that the pace of change in the technological change is so fast, policy just can't keep up with that. And so be very careful not to specifically target that.

And only one last thing—I can't resist this—this is not an industry chart, I can assure you, and having been on the other side in Government, only Government could draw a chart like that. That's just a description of the number of agencies that have jurisdiction or claim jurisdiction within the Federal Government on this issue, and being able to have a little interagency cooperation and clearing, I think, would go a long way, and also working with the private sector—we're down here at the bottom someplace—and there needs to be some real focus to address that issue in the long term.

Mr. SMITH. Thank you, Mr. McCurdy. I think you're right about not being specifically targeted on certain technology, because that will in turn become outdated.

I'm going to ask the—oh, we have 3 Members left—if you all will limit yourself to 3 minutes, we can finish before the series of votes, or we can come back. But let's start, and let's assume we can get through the questions with 3 minutes allowed for each Member, and Ms. Jackson Lee from Texas is recognized for her questions.

Ms. JACKSON LEE. Thank you very much, Mr. Chairman. Let me thank the witnesses for their testimony. I think they were very thorough, and in light of the restraints that we've voluntarily placed upon ourselves, let me say to you that I do have a great concern with the competing interests, of a question of child pornography that one can find invading on the Web and on the Internet, the violations and the, if you will, misuse of your business sites and the kind of unfortunate results that can come of that, and then of

course, the privacy question, of being able to protect the personal information that is shared with you, particularly if it's shared anonymously and shared by legitimate business interests or an adult.

I'd like to go to you, Mr. McCurdy, and thank you very much for joining us. Thank you for your leadership and the other members. How do we protect the personal—the personal information that you receive, the various businesses receive, from individuals who are sending it for a particular reason?

Mr. MCCURDY. Well, thank you, Congresswoman, and that's a very good question. I think there's been a lot of progress made on the privacy front. This issue has arisen, and I think there's been a great deal of debate. Each of us here have been engaged in this for quite some time. And you see progress—I don't know if at home in your mail you've been recently—from your bank you're getting statements of their privacy policy, and a lot of people are adopting those, and on the websites there's provisions for that as well.

This is always an issue of balance and is going to be. We can have privacy, but you can't have privacy without security, so security is where you really need to focus first. Now, you can have security and violate policy and privacy, but you really—the two have to match. And from our perspective—and I'm not talking about the—since we've had computers, there have been those who know how to get inside computers, including this Government. And some of my previous experience on the Intelligence Committee, I can assure you that that's a fact. The private sector I think has done a good job of trying to secure the information. The issue that comes up here is if we are to collaboratively have worked together, we need to be able to share information that's generated from different sources, and that should not be subject to public disclosure in some way, and that's why the FOIA legislation is so critical.

So, one, I think progress has been made on privacy. We would hope that Congress not overreact and go too far on the privacy front, because I think there is a sufficient degree of movement there, and at the same time that they work with us on the overall security issue of being able to share this information because ultimately it's the consumers and the market's going to determine whether or not this is a success, and if they feel that this is threatened, their privacy's threatened, they won't use our products.

Ms. JACKSON LEE. Thank you very much, Mr. Chairman.

Mr. SMITH. Thank you, Ms. Jackson Lee. Mr. Goodlatte, I know you're on your way out the door. Do you want to ask a quick question?

Mr. GOODLATTE. Yeah. The area that I wanted to follow up in, Mr. Kruger, I have a series of questions I've given the Chairman that I would ask that you respond to in writing. We don't have enough time to do that. But if you could comment briefly on the enforcement of the NET Act, No Electronic Theft Act, thus far, it would be very helpful to us to know what has been happening in terms of the Justice Department fighting piracy on the Internet. This is legislation that Congress passed a few years ago, that cracks down on this multibillion a year problem, and I don't think we're making as much progress as we would like. We asked the At-

torney General about this last week. We'd like to hear your perspective.

Mr. KRUGER. Congressman Goodlatte, well, first I'd like to recognize you as one of our champions on this issue. You have certainly helped the industry in the past.

On the NET Act specifically, we're encouraged but very modestly encouraged by some recent trends that are reported on the Department of Justice website. From January through May, there were 10 prosecutions involving software piracy. Two of those, I think, fall under the NET Act, and while that's hardly a torrent of activity, it compares very favorably to two prosecutions all of last year, and one in 1999. So I think we're seeing a modest uptick.

And in addition, as I mentioned during my oral testimony, there was a conviction last month by a Federal jury, after the first jury trial under the NET Act of a member of the notorious Pirates With Attitude software ring in Chicago. So we finally have won after a jury trial. And I think that's an indication of something. I think when a jury speaks, it adds sort of public condemnation to what we've already had, which is congressional statements and prosecutorial statements to that effect.

So I think there is some progress being made, but we would urge this Committee to continue to exercise its oversight to ensure that progress continues.

Mr. SMITH. Thank you, Mr. Goodlatte. Mr. Goodlatte, do you want to have these questions submitted to Mr. Kruger?

Mr. GOODLATTE. Yes. If the Committee would do that, and he would respond in writing, I would appreciate that.

Mr. SMITH. We have some questions we would like you to answer, if you would, in writing, get back to us within 2 weeks.

Mr. KRUGER. Be happy to do that.

Mr. SMITH. Also, without objection, the complete statement of the gentlewoman of Texas, Ms. Jackson Lee, will be made a part of the record.

[The prepared statement of Ms. Jackson Lee follows:]

PREPARED STATEMENT OF THE HONORABLE SHEILA JACKSON LEE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

I want to thank Chairman Smith and Ranking Member Scott for convening an oversight hearing on *"Fighting Cybercrime—Efforts by Private Business Efforts Interests."* This is the third of a four part hearing series on Cybercrime. The first hearing held on June 12, 2001, covered state and local efforts to combat Cybercrime. The second hearing focused on federal efforts to combat Cybercrime. The hearing today addresses industry efforts to combat Cybercrime.

As lawmakers and concerned citizens, we are painfully aware of the dilemma posed by Cybercrime. The role played by industry is very critical to our efforts to stem continuing abuse and threats against private business and even government. At the hearings on Cybercrime issues, both the companies that these laws would protect, and privacy/civil liberties advocates for users of electronic services, sounded alarms about the adverse impact that could result from law enforcement that is too heavy-handed. For example, testimony revealed that the laws on the book may be more than is needed in that judges, juries and even prosecutors were balking in some cases at finding young hackers guilty because of the necessity of a 6-month mandatory minimum sentences upon conviction.

I have often expressed my reluctance to support mandatory minimums in other settings. But the primary concern about legislative efforts to combat Cybercrime was their impact on traditional exceptions of privacy and protections of civil liberties. We cannot ignore these concerns in our battle against Cybercrime.

Accordingly, we have considered a number of legislative remedies to address this serious matter, including increasing the penalties for invasions into stored commu-

nications, forfeiture of any property used or intended to facilitate a crime, making computer crime a RICO predicate, and other valuable measures.

As the industry contemplates crafting solutions, there are the major laws setting privacy standards for government interception of communications and access to subscriber information. These include the federal wiretap statute ("Title III"), 18 USC 2510 et seq., requiring a probable cause order from a judge for real-time interception of voice and data communications; the Electronic Communications Privacy Act of 1986 (ECPA), 18 USC 2701 et seq., setting standards for access to stored electronic communications and transactional records; and the pen register which governs real-time interception of "the numbers dialed or otherwise transmitted on a telephone line."

We continue to revisit the same concerns regarding privacy and civil liberties in these Cybercrime hearings. That is partly because the field of electronic communications is a developing one. While there is a role for law enforcement in enforcing these laws, prudence must be utilized. Additionally, there is a growing list of law enforcement horror stories demonstrating that the electronic communications industry be given a full opportunity to develop effective security measures to ensure protections of privacy.

Like many of you, I recognize that horror stories such as a recent Texas case involving confiscation of all of one business' computers based on an accusation of electronic communications sabotage by a rival business reflect the dangers of too much involvement of law enforcement. The accused business, against which charges were eventually dropped, lost months of business while incurring legal and other costs to get its equipment back.

Given the global nature of the information age, there is a need for coordination of law enforcement efforts between federal, state and local entities, and more resources from the federal government to state and local entities for training, equipment, and other needs, to enable them to keep up with criminals who operate in the Cybercrime environment.

Mr. Chairman, I look forward to the testimony today regarding the industry's role in curbing the threat of Cybercrime in all possible permutations. We cannot do this without your input. Thank you.

Mr. SMITH. And we'll look to Mr. Delahunt for his questions.

Mr. DELAHUNT. I'll be very brief, Mr. Chairman, and——

Is it a fair statement the say that the problems as you perceive them in terms of Government response are jurisdictional issues? I think that might have been part of the rationale that Mr. McCurdy showed us the diagram. And what you would say, not inadequate, but insufficient resources at this point in time, or do you think that in terms of—and I do concur with Mr. McCurdy as far as insuring that whatever substantive legislation passes, that we be careful not to try to create technology-specific bills. Otherwise, we're getting ourselves, I think, into a quagmire. Mr. Miller.

Mr. MILLER. Mr. Delahunt, I think it's important to note that the Bush Administration has a effort under way now to try to deal with the problem that Mr. McCurdy identified in his chart. There is an effort under way to try to coordinate the efforts better. ITAA itself has advocated the creation of a Federal czar, similar to the role John Koskinen played in Y2K. I'm not sure the Administration's going to go for that, but we are encouraged by the fact that under the national security adviser——

Mr. DELAHUNT. You're suggesting a tech czar as well as a——

Mr. MILLER. Absolutely. Not a big staff, the same kind of role that Mr. Koskinen played, which was a whip hand that had the backing of the President.

Mr. DELAHUNT. Analogous to the drug czar.

Mr. MILLER. Exactly. But if they won't go that far, at least what we hear from the National Security Council, from Mrs. Rice and the Department of Commerce, is there is a sophisticated——

Mr. DELAHUNT. One other just quick question. You referred to the international dimension here, and I think that's something that we have to recognize. What is happening internationally? Is there planning in terms of a possible convention that the United States could promote with an eventual treaty to be considered by the various governments?

Mr. MILLER. That's what the Council of Europe has been trying to develop, Mr. Delahunt. We think much of that is very positive. There are still a few problematic areas that industry is trying to work with. The U.S. is not a member of the Council of Europe, but they do have advisory status, and the Department of Justice has provided a lot of input, and we're hopeful that that final treaty can be something that industry would support.

Mr. DELAHUNT. I think that's something, Mr. Chairman, that we should take note of.

Mr. MCCURDY. The point is, it is far from perfect. If anything, it is fundamentally flawed at this point, and I would like—we encourage international cooperation, but that treaty is not the answer right now. So there are—you know, it's moving, but we have direct input other than an advisory role, and so I think there—if we're really going to work on a much broader cooperative role internationally the U.S. needs to take a more——

Mr. DELAHUNT. You encourage——

Mr. MCCURDY. I think the Administration understands this, but again, this is not just a cyber crime or national security issue. We need to focus on the economic security aspect of this.

Mr. MILLER. If I could——

Mr. SMITH. Thank you, Mr. Delahunt. Mr. Harris (sic), I'm afraid we're going to have to move on.

Thank you all for your testimony. It's been very, very helpful. I might add—and I didn't go into much detail today—but I've seen examples of all the different types of cyber crime you talk about, back home in my district as I visited various high-tech companies. And I've seen $500, you know, pieces of software duplicated for 5 cents in Korea, sold on the underground market here. I've seen my own website in Congress—now, you talk about a real threat, Harris, it's when a member's website is broken into, and no telling what embarrassing information might be put there to distance the member from the constituency, which is not a good thing to have happen.

Anyway, regardless of the type of cyber crime, it's a real threat. It's just as serious as physical crime, and we appreciate your help in making suggestions to combat it.

So thank you all for being here, and we stand adjourned.

[Whereupon, at 10:54 a.m., the Subcommittee was adjourned.]

APPENDIX

STATEMENTS SUBMITTED FOR THE HEARING RECORD

PREPARED STATEMENT OF THE COUNCIL OF EUROPE DRAFT CONVENTION ON CYBER-CRIME FROM THE WORLD INFORMATION TECHNOLOGY AND SERVICES ALLIANCE (WITSA)

WORLD INFORMATION TECHNOLOGY AND SERVICES ALLIANCE (WITSA) STATEMENT ON THE COUNCIL OF EUROPE DRAFT CONVENTION ON CYBER-CRIME

November 2000

The World Information Technology and Services Alliance (WITSA) welcomes the opportunity to participate in the crucial dialogue on how to most constructively and effectively enforce criminal law in the increasingly international law enforcement environment fostered by the Internet and other information networks. Because efforts to improve law enforcement in the digital environment can have both positive and negative effects on the health and growth of the international information economy, it is essential that such efforts be based on the close consultation and cooperation between government, industry and civil society that can generate consensus among all interested parties, and ensure that new measures are carefully crafted and effectively applied.

The evolving information age requires a minimalist approach to regulation of information technology and information systems, particularly in the criminal realm. The Internet and information technology thrive in a relatively unconstrained environment which fosters rapid innovation and free dissemination of information. Moreover, since a principal function served by the Internet is to enable the free exchange of information, efforts to target regulation specifically at activities on the Internet touch on sensitive issues of individual liberty as well as cultural tradition. Criminal law must be available to prevent and counteract harmful illegal activity on the Internet, but regulation specifically aimed at the information sector can and should be very narrowly tailored.

The majority of what are termed "cyber-crimes" is really violations of long-standing criminal law, perpetrated through the use of computers or information networks. The problems of crime using computers will rarely require the creation of new substantive criminal law; rather, they suggest need for better and more effective means of

international cooperation to enforce existing laws. On the other hand, there are new and serious problems posed by attacks against computers and information systems, such as malicious hacking, dissemination of viruses, and denial-of-service attacks. Such attacks should be effectively prohibited, wherever they may originate. At the same time, it bears remembering that often the most effective way to counter such attacks is to quickly deploy technical countermeasures; therefore, to the extent that well-meaning but overbroad criminal regulations diminish the technical edge of legitimate information security research and engineering, they could have the unintended consequence of actually undermining information security.

Although WITSA supports the objectives of improving international law enforcement cooperation and mutual legal assistance to keep pace with the increasingly international environment, it has serious concerns with many of the provisions of the draft cyber-crime convention. In its current form, the draft convention could impose burdensome data preservation requirements on Internet service providers (ISPs); make ISPs liable for third party actions; and restrict legitimate activities on the Internet.

I. World Information Technology and Services Alliance (WITSA)

The World Information Technology and Services Alliance (WITSA) is a consortium of 41 information technology (IT) industry associations from economies around the world (list attached). As the global voice of the IT industry, WITSA is dedicated to:

- advocating policies that advance the industry's growth and development;
- facilitating international trade and investment in IT products and services;
- strengthening WITSA's national industry associations through the sharing of knowledge, experience, and critical information;
- providing members with a vast network of contacts in nearly every geographic region of the world; and
- hosting the World Congress on IT, the only industry sponsored global IT event.

Founded in 1978 and originally known as the World Computing Services Industry Association, WITSA has increasingly assumed an active advocacy role in international public policy issues affecting the creation of a robust global information infrastructure, including:

- increasing competition through open markets and regulatory reform;
- protecting intellectual property;
- reducing tariff and non-tariff trade barriers to IT goods and services; and safeguarding the viability and continued growth of the Internet and electronic commerce.

More information on WITSA can be found online at http://www.witsa.org.

II. Burdensome Record Keeping

On May 15, 2000, the Group of Eight (G8) countries held a cybercrime meeting in Paris in an effort to start a discussion on combating Internet crime and closing "'digital havens' that protect hackers'." One of the issues discussed at that meeting was the Council of Europe's draft convention. WITSA issued a statement to the G-8 in opposition to controversial provisions which permitted some governments to interpret Article 15 (16) (Expedited preservation of data stored in a computer system) and Article 16 (17) (Expedited preservation and disclosure of traffic data) as requiring parties to mandate that ISPs preserve and maintain the integrity of traffic data for Internet transmissions for

significant periods. Even if this was interpreted as only requiring prospective preservation on demand, it could impose burdensome and intrusive requirements on ISPs. WITSA encourages governments to avoid imposing new requirements on ISPs that result in significant financial burdens on their operations. Such added costs will ultimately affect the access costs of end users, and may negatively impact the growth of Internet usage.

Further, even if information of this sort could be collected and stored, this requirement raises serious privacy concerns. Given the debate going on around the world on the need to protect the privacy of Internet users, it makes little sense to require ISPs to collect and store more information than ever before.

WITSA believes revisiting this provision in consultation with the IT industry would benefit all the parties concerned.

III. Liability for Third Party Actions.

The draft convention requires parties to enact a variety of criminal laws (Articles 2-10), and then to criminalize aiding and abetting the commission of those offenses (Article 11). Because these offenses are committed via ISPs' systems, ISPs properly are concerned that they may be found to have aided and abetted the commission of the offenses. This is particularly the case with respect to Article 10, concerning copyright. Balancing the rights and interests of copyright holders and Internet service providers has been the subject of long and intensive negotiation in many countries, yielding hard-won and carefully crafted compromise legislation providing detailed, workable guidelines to address the problem of infringement. Under the text of the CoE treaty, an ISP may receive a vague notice from a content provider that somewhere in the ISP's service some infringing material has been uploaded by a subscriber.

WITSA believes it is critical that liability not be imposed on ISPs for the criminal acts of third parties using their facilities.

IV. Restriction of Legitimate Activities

The Internet flourishes in an environment in which regulatory minimalism fosters innovation and initiative. Accordingly, it is of particular concern that some offenses defined in the text are drafted so broadly that they might prohibit legitimate activities. For example, Article 2 requires a prohibition on access to a computer system "without right." Would this prohibit the use of "cookies"? Would it preclude or inhibit third party testing and evaluation of software, security systems or reverse engineering? Would this criminalize the use of search engine bots? Would this preclude instant messaging between competing ISPs? Clearly, these sorts of activities should not be treated as criminal offenses -- certainly not at this early stage of the Internet's development. Doing so will not only harm ISPs; it would also retard the growth of the Internet, to the detriment of hundreds of millions of users.

WITSA supports language that carefully and clearly defines harmful illegal behavior and does not criminalize legitimate activity.

Conclusion

The international enforcement problems implicated by crime using information systems, as well as the substantive problem of crimes committed against information systems, require close cooperation and dialogue between government and the information industry. The reactions to the draft Council of Europe Convention on Cyber-Crime indicate that this important process is just beginning. WITSA is committed to participation in that dialogue, and to reaching a consensus on carefully tailored measures that will both support effective international law enforcement and foster continued growth and innovation in the information sector.

The Statement is available online at http://www.witsa.org/papers/COEstmt.pdf. A Press release is available at http://www.witsa.org/press/COEpr.pdf.

The World Information Technology and Services Alliance (WITSA)

WITSA consists of the national information industry representative bodies from around the world. Its role is to develop public policy positions on issues of concern to the information industry and present these positions to governments and international organizations. WITSA members are:

Argentina	Cámara de Empresas de Software y Servicios Informáticos (CESSI) URL: http://www.cessi.org.ar / E-mail: camara@cessi.org.ar
Australia	Australian Information Industry Association (AIIA) URL: http://www.aiia.com.au/ E-mail: aiia@aiia.com.au
Bangladesh	Bangladesh Computer Samity (BCS) URL: http://www.samity.org E-mail: samity@dhaka.agni.com
Brazil	Sociedade de Usuários de Informática e Telecomunicações - Sao Paulo (Sucesu-SP) URL: http://www.sucesusp.com.br E-mail: sucesusp@sucesusp.com.br
Canada	Information Technology Association of Canada (ITAC) URL: http://www.itac.ca/ E-mail: info@itac.ca
China, Taipei	Information Service Industry Association of China, Taipei (CISA) URL: http://www.cisanet.org.tw/english/index.html /E-mail: cisa@mail.cisanet.org.tw
Colombia	Colombian Software Industry Federation (FEDESOFT) URL: www.fedesoft.org E-mail: proyectos@cati.org.co
Czech Republic	Association for Consulting to Business (Asociace Pro Poradenství v Podnikání - APP) URL: http://www.asocpor.cz/ E-mail asocpor@asocpor.cz
Ecuador	Association Ecuatoriana de Tecnologia de Informacion y Servicios (AETIS) aetis@usa.net
Egypt	The Co-operative Society for Computers of Egypt (CSCE) E-mail: jumboco@starnet.com.eg
Finland	Information Technology Services Association (Tietotekniikan Palveluliitto - TIPAL) URL: http://www.tipal.fi/index.html E-mail: tipal@tipal.fi
France	Syntec Informatique URL: http://www.syntec-informatique.fr/ / jpeybert@syntec-informatique.fr
Germany	German Association for Information Technology, Telecommunications and New Media (BITKOM) URL: http://www.bitkom.org/ E-mail: bitkom@bitkom.org
Greece	Federation of Hellenic Information Technology and Communications Enterprises (SEPE) URL: http://www.sepe.gr / E-mail: sepe@compulink.gr
Hong Kong	Hong Kong Information Technology Federation (HKITF) URL: http://www.hkitf.org.hk/ E-mail: mok@hknet.com
India	National Association of Software and Service Companies (NASSCOM) URL: http://www.nasscom.org/ E-mail: nasscom@nasscom.org
Israel	Israeli Association of Software Houses (IASH) URL: http://www.iash.org.il/ E-mail: software@industry.org.il
Italy	Associazione Nazionale Aziende Servizi Informatica e Telematica URL: http://www.anasin.it/ E-mail: Anasin@anasin.it
Japan	Japan Information Technology Services Industry Association (JISA) URL: http://www.jisa.or.jp/ E-mail: info@jisa.or.jp
Lithuania	Association of the information technology, telecommunications and office equipment companies of Lithuania (INFOBALT) URL: www.infobalt.lt E-mail: office@infobalt.lt

Malaysia	Association of the Computer And Multimedia Industry Malaysia (PIKOM) URL: http://www.pikom.org.my E-mail: info@pikom.org.my
Mexico	Asociación Mexicana de la Industria de Tecnologías de Información (AMITI) AMITI: http://www.amiti.org.mx/ E-mail: amiti@amiti.org.mx
Mongolia	Mongolian National Information Technology Association /E-mail: enkhbold@mtu.edu.mn
Morocco	L'Association des Professionnels de L'Informatique de la Bureautique et de la Telematique (APEBI) / http://www.apebi.org.ma/ E-mail: apebi@apebi.org.ma
Netherlands	Federation of Dutch Branch Associations in Information Technology (Federatie Nederlandse IT - FENIT) URL: http://www.fenit.nl/ E-mail: bureau@fenit.nl
New Zealand	Information Technology Association of New Zealand (ITANZ) URL: http://www.itanz.org.nz/ E-mail: info@itanz.org.nz
Northern Ireland	Momentum - The Northern Ireland ICT Federation URL: http://www.sif.co.uk E-mail: billy@sif.co.uk
Norway	ICT Norway (IKT Norge) / http://www.ikt-norge.no/ E-mail: bt@ikt-norge.no
Poland	Polish Chamber of Information Technology and Telecommunications (Polska Izba Informatyki i Telekomunikacji - PIIiT) / http://www.piit.org.pl/ Email: piit@ikp.atm.com.pl
Portugal	Associação Portugesa das Empresas de Tecnologias de Informação e Comunicações (APESI) E-mail: apesi@treal.pt
Republic of Korea	Federation of Korean Information Industries (FKII) URL: http://www.fkii.or.kr/ E-mail: FKII@chollian.net
Romania	Association for Information Technology and Communications of Romania (ATIC) URL: http://www.atic.org.ro E-mail: Vlad.Tepelea@algoritma.ro & atic@softnet.ro
Singapore	Singapore Information Technology Federation (SITF) URL: www.sitf.org.sg E-mail: sitf@sitf.org.sg
South Africa	Information Industry South Africa (IISA) URL: http://www.ita.org.za E-mail: ita@ita.org.za
Spain	Asociación Española de Empresas de Tecnologías de la Información (SEDISI) URL: http://www.sedisi.es E-mail: info@sedisi.es
Sweden	The Association of the Swedish IT and Telecom Industry (IT-Företagen) URL: http://www.itforetagen.se/ E-mail: info@itforetagen.se
Thailand	The Association of Thai Computer Industry (ATCI) URL: http://www.atci.or.th/ E-mail: Info@ATCI.or.th
United Kingdom	Computing Services & Software Association (CSSA) URL: http://www.cssa.co.uk/ E-mail: cssa@cssa.co.uk
United States	Information Technology Association of America (ITAA) URL: http://www.itaa.org/ E-mail: jmcwilliams@itaa.org
Venezuela	CAVEDATOS - Venezuelan Chamber of IT Companies URL: www.cavedatos.org E-mail: cavedato@telcel.net.ve
Zimbabwe	Computer Suppliers' Association of Zimbabwe (COMSA) / comsa@csz.icon.co.zw

MATERIAL SUBMITTED FOR THE HEARING RECORD

POST HEARING QUESTIONS FOR MAY 24,2001, HEARING ON FIGHTING CYBER CRIME - HEARING 1 OF 3: EFFORTS BY STATE AND LOCAL OFFICIALS

(Director Ronald R. Stevens, of the N.Y. State Police Computer Crimes Unit)

In your written testimony, you state that the New York State Crimes Against Children Task Force has received just over $250,000 in Federal grant money from the Office of Juvenile Justice and Delinquency Prevention in each of the past three years.

a. Can you tell us how this money was used to fight Internet crimes against children?

b. How effective was this program?

c. How could this program be improved?

According to your testimony, New York State has over 500 local police departments with many of these being small rural departments with staffing levels of less than 10 officers.

a. What kinds of issues are these small rural departments facing that the larger metropolitan departments are not?

b. What is New York doing to help the rural departments investigate cyber crimes.

(Question 1.a.) **Can you tell us how this money was used to fight Internet crimes against children?**

Answer:

February of 1999, the New York State Crimes Against Children Task Force was formed with primary responsibilities including training for law enforcement, promoting public education, providing investigative and prosecutorial assistance and forensic analysis of computers seized as evidence. The grant monies awarded by the Office of Juvenile Justice and Delinquency Prevention were used to provided the salaries for one task force position from each of the three participating agencies. The first year of the grant emphasis was placed on education, training and public awareness. Public service announcements were conducted, parent and child safety booklets were published and printed, and statewide training was conducted. Computer equipment was purchased to conduct undercover activities and forensic analysis of computer evidence. Undercover backdrops were established with post office boxes and drop boxes, Internet connections and telephone hookups. An "800" number and an on-line complainant system(established within the NYSP website) to intake complaints about Internet crimes against children.

Additionally, in the second and third year of the grant a fourth position was established to assist with the criminal investigations as a analytical specialist.

(Question 1.b.) **How effective was this program?**
Answer:

This program has been extremely effective. With regards to first year emphasis on training, education and public awareness. The three member ICAC task force along with support staff from each agency held 8-one day training sessions and 5-four day advanced sessions. These training sessions reached more than 1650 law enforcement officers and 88 prosecutors, lectured to more than 295 social workers, 400 school children and administrators and handed out more than 33,000 parent and child safety pamphlets.

The following is an illustration to support the investigative effectiveness of this program. On May 11, 2000 members of the New York State ICAC task force, along with the United States Postal Inspection Service and FBI, executed a federal search warrant at a Homer, New York residence. The Cortland County resident was subsequently arrested for receiving child pornography via the U.S. mail. During the execution of the Court ordered Search Warrant an active hydrophonics marihuana growing operation was located within the defendant's bedroom. 68 marihuana plants, marihuana grow lights and paraphernalia, a computer system, and printed images of child pornography were seized from the residence.

The case centered on the defendant having purchased child pornography from an Internet Crimes Against Children member in an undercover capacity on the Internet. Local police and school authorities had developed information the defendant may have been selling marihuana to school age youths and the defendants residence was located less than 1000 feet from the local high school.

The defendant, age 36, was sentenced to 6 years 2 months in a federal prison for Receiving Child Pornography, Possession of Child Pornography and the Manufacturing of Marihuana.

(Question 1.b.) **How could this program be improved?**
Answer :

The concept of networking state and local law enforcement agencies and then affording them the same tools to counter the emerging threat of offenders using the Internet or other online technology to sexually exploit children can not be improved on.

The program could be improved through continued funding to Office of Juvenile Justice and Delinquency Prevention to support this program so each state could be awarded a like task force program and those that are already established could receive additional support to fight this crime.

Though this task force concept is a good initial step, additional staffing is required to continue the education process of children, parents and law enforcement. Also additional law enforcement and prosecutorial personnel are needed to continue the online investigations, arrests and prosecutions of child sexual predators. With the additional arrests comes the forensic personnel needed to analysis the computers and related evidence used to commit these crimes.

(Question 2.a.) **What kinds of issues are these small rural departments facing that the larger metropolitan departments are not?**
Limited resources/lack of dedicated manpower, hardware, equipment and training

(Question 2.b.)**What is New York doing to help the rural departments investigate cyber crimes.**

Our plan with OFT, training, free forensic analysis, field support, search warrant support,

OFFICE OF THE ATTORNEY GENERAL · STATE OF TEXAS
JOHN CORNYN

June 21, 2001

Subcommittee on Crime
Attn: Veronica Eligan
207 Cannon House Office Building
Washington, D.C. 20515

Re: Hearing Concerning the Oversight on Fighting Cyber Crime - Hearing 1 of 3: Efforts by State and Local Officials.

Dear Ms. Eligan:

Enclosed please find my responses to the post hearing questions regarding the above-referenced hearing held on May 24, 2001. I do not have any edits to the transcript of my testimony.

Thank you for your assistance.

Sincerely,

Michael T. McCaul
Deputy Attorney General for Criminal Justice

MTM/kh

Enclosure

cc: Congressman Lamar Smith, Chairman, Subcommittee on Crime
Attorney General John Cornyn

Subcommittee on Crime

Hearing on Fighting Cyber-Crime, May 24, 2001: Post-Hearing Questions for Michael T. McCaul, Deputy Attorney General for Criminal Justice
Office of the Attorney General, State of Texas

1. *You stated that according to the FBI, child pornography was virtually extinct prior to the advent of the Internet and now with increased Internet usage child pornography is on the rise again. You then provided some very disturbing statistics with regard to child pornography and the Internet.*

   a. *How can the Federal government help local law enforcement in efforts to stop on-line child pornography?*

Federal regulation requiring Internet Service Providers (ISPs) to capture and maintain Internet Protocol Addresses (IP Addresses) and Internet activity records for its users for a specified amount of time, at least twelve months, would be invaluable in helping law enforcement officers to track and trace on-line criminals. Today, each ISP decides for itself for how long to maintain IP Addresses and user activity logs, and indeed, whether to capture such information at all. Similar regulations applied to web pages would also be very helpful for law enforcement efforts.

Another way in which the Federal government can help local law enforcement efforts is to fund more regional computer forensics labs, and make their services available at no cost to local law enforcement agencies. Computer forensics require tremendous expertise and take time. Often, a case cannot proceed until forensics are completed. Increasing the number of computer forensics labs available to law enforcement agencies would greatly increase our and other states' ability to catch and prosecute Internet criminals.

   b. *Are there any statutory gaps of which you are aware that are preventing law enforcement from adequately addressing this growing problem?*

The primary statutory gap, which I mentioned in my testimony, is that subpoenas from one state are not enforceable in another state. In many instances this may not be an insurmountable problem: service can be affected through the Secretary of State when an ISP or web page has an actual presence in the state. There are many more instances, however, where the ISP or web page has no presence in the state where the crime was committed and law enforcement personnel will have to go through the difficult and lengthy process of getting a subpoena or court order issued through a jurisdiction in a different state. Legislation requiring ISP's to comply with out of state process is needed to resolve this problem.

In addition, there appears to be a gap in the language of the Electronic Communications Privacy Act, 18 U.S.C. § 2701 *et seq.*, the primary federal law proscribing the method of

obtaining records from ISPs. Title 18, United States Code, Section 2703(d) appears to allow only federal judges – to the exclusion of state judges -- to issue orders requiring ISPs to disclose transactional information regarding a user's internet activity. *See* 18 U.S.C. §§ 2703(d) & 3127(2)(A). This is inconsistent with other provisions of the statute which allow both federal and state judges to issue search warrants or subpoenas for records from ISPs. *See* 18 U.S.C. §§ 2703(a) & (b)(A). These provisions should be harmonized by amended section 2703(d) to allow state judges to issue orders requiring ISPs to disclose to law enforcement transactional records regarding a subscriber's Internet activity.

2. *Do cyber crime investigations require the cooperation of the Internet Service Providers? If so, could you explain whether that cooperation is adequate or how you think it could be improved.*

Cyber crime investigations require the cooperation of ISPs because records involving Internet usage are one of the primary tools for tracing on-line criminals, and those records are generally captured and maintained by ISPs. Cooperation varies widely from ISP to ISP. Some, such as AOL, cooperate regularly with law enforcement subpoenas, but maintain records only for limited periods of time. Other ISPs refuse to comply with subpoenas and insist on receiving a signed court order before disclosing subscriber information. Cooperation could be enhanced if ISP's were required to maintain Internet usage records for a set period of time, preferably at least 12 months.

3. *Please explain the types of challenges your office has faced in dealing with cyber crime?*

Time limitations are one of the main challenges the Texas Internet Bureau has faced in dealing with cyber crime. IP Addresses are typically maintained only for limited periods of time. If a crime is reported late, or if law enforcement officials must trace criminal activity through several different ISP's, or the connections cross several jurisdictional lines, the evidence linking the perpetrator to the crime can be erased by an ISP or a web page before the police are in a position to request it. Occasionally, an ISP's legal staff is not aware of the technical capabilities of their systems. This may cause the ISP's to respond that they do not have the evidence sought. In such cases, persistence is usually the key to success. Again, however, persistence can take time, and time can sometimes be costly. A third challenge is a reticence on the part of private industry and companies to report cyber crimes such as hacking for fear of harming their reputation, alerting the "hacker" community to a weakness in their security system, or out of a belief that traditional law enforcement can offer them no help.

4. *According to the Federal Bureau of Investigation's Internet Fraud Complaint Center, New York and Texas are among the States receiving the most complaints about Internet Fraud.*

   a. *Would you agree?*

Since I am not familiar with how the IFCC calculated its statistics, I do not know if Texas receives more complaints per capita, or over all, or both. I do note that the Texas Internet Bureau is receiving a large number of complaints regarding online fraud, and it would not surprise me if Texas were one of the leaders in this category.

b. If this is the case, why do you believe that Texas has more complaints than most of the other states? Are Texas citizens better at reporting fraud or are they more often targeted?

Texas is a large state and many of our citizens are technologically savvy. Technology has recently replaced oil and gas as the largest segment of our economy. I believe Texas citizens are being targeted and that law enforcement in our state has done a good job of informing the public of where and how to report these offenses. Thus, I am not surprised that Texas ranks near the top of the list in terms of on-line fraud.

c. Is this one reason you created the Internet Bureau?

Every type of Internet crime is a cause of great concern for Texas and Attorney General John Cornyn and led to his creating the Texas Internet Bureau. Attorney General Cornyn has consistently emphasized protecting those that cannot protect themselves, and thus many of the Internet Bureau's investigations focus on cyber crimes that target children -- the online distribution of child pornography and exploitation of children. The Internet Bureau also aggressively investigates and prosecutes fraud that occurs on the Internet.

5. In your testimony, you mention that retention of technically trained law enforcement officers is a problem. What efforts is Texas undertaking to resolve or lessen this problem?

I do not have specific statistics as to what local law enforcement agencies around the state are doing to train and retain their technically savvy law enforcement officers. I do know, from anecdotal evidence, however, that many of our local Police Departments and Sheriff's Officers are setting aside officer positions for computer forensics specialists and computer crime specialists. In addition, the Texas Internet Bureau has proposed starting a Detail/Intern program in which local police officers and sheriff's deputies from around the state will spend 6-9 months at the Internet Bureau working exclusively on Internet crimes and receiving valuable training and experience. At the end of their detail they will return to their local agency. In addition, the lawyers and police officers at the Internet Bureau have conducted numerous training sessions for law enforcement throughout the state of Texas and plan on hosting a computer crimes school in Austin in early 2002.

6. The Federal Computer Crime Enforcement Act was signed into law last year. That law created a grant program to assist State and local law enforcement agencies in their law enforcement efforts against computer crime. The law

authorizes $25 million a year from FY 2001 through 2004. Do you believe that law will help you in your efforts and is it enough?

I believe the Act will be very helpful, if funds are actually appropriated. Currently, no funds have been allocated to the grant program and so it exists in name only. The Internet Bureau receives far more referrals than its six investigators can handle. New funds could be used to hire and train additional investigators. $25 million per annum is not much to fund efforts across the nation. Technology is expensive and always evolving. High tech crime units must keep pace with new technology if they are to effectively investigate crimes utilizing it. In short, $25 million is not enough. More funding is needed if states are to develop effective cyber crime fighting initiatives.

-----Original Message-----
From: cassilly, joseph [mailto:jicassilly@co.ha.md.us]
Sent: Thursday, August 16, 2001 4:54 PM
To: Sokul, Beth
Subject: Answers to Local prosecutors questions

JOSEPH I. CASSILLY
STATE'S ATTORNEY
JAY E. ROBINSON
DEPUTY STATE'S ATTORNEY
DIANA A. BROOKS
Circuit Court Division
DEPUTY STATE'S ATTORNEY
STATE'S ATTORNEY FOR HARFORD COUNTY
COURTHOUSE
20 WEST COURTLAND STREET
BEL AIR, MARYLAND 21014
Bel Air Telephone (410) 638-3500
Baltimore Telephone (410) 879-320
(410) 638-3242
Fax (410) 838-2023

August 16, 2001

MEMO

TO: Beth Sokul

FROM: Joe Cassilly

I apologize for not going into greater detail with some of my answers but I thought that it was important to get these right back to you. If you need more on any question my e-mail is jic@co.ha.md.us.

1. (a.) When I said that I had worked with all of these agencies I meant in separate investigations. I do not know how the various law enforcement agencies would work together to advance the same case. I can say that some of the ISP's are very cooperative with local law enforcement and others less so.

1. (b.) One of my suggestions is the creation of regional, inter-agency computer forensic labs that would bring togehter examiners and investigators from different agencies and

different levels of government.

1.(c.) I think that the Federal level of cooperation is very inconsistent around the country. In other words if the FBI agent in charge is outgoing and recognizes the importance of the locals you get cooperation. On the other hand, if everyone is guarding their turf and their egos you o not.

2. I told this story to emphasize the urgency of getting records from other States and the distances that information travels to other witnesses. One solution would be the establishment of 24-hour law enforcement hot lines so that the police would not have to wait for normal business hours.

3. I think that distance and privacy concerns will be the greatest challenges facing conventional law enforcement and the court system. In the traditional criminal investigative paradigm a police officer responds to a crime scene, interviews and takes statements from the victim and witnesses, collects evidence and arrests a defendant. In a cybercrime, the crime scene is somewhere in cyberspace, the victim may be next door or in the next State, the same for the suspect. The witness may be someone you never see and communicate with by e-mail. The evidence may be in a micro-disk that you can't look at without violating three Federal laws. The prosecutor faces the same problem of assessing whether he can prosecute a crime.

Much of this has to be solved by training and resources. Prosecutors must have the resources to keep attorneys who are experienced with these cases working in prosecution and not lose them to better paid positions in the private sector. Second, they need training that is directed to prosecutors and they need resource attorneys. Resource Attorneys would be former prosecutors or prosecutors on loan from their regular jobs who are paid to keep up on the latest trends and laws, problems and solutions of cybercrime and bring them to the attention of the trial attorneys or be available to take questions from prosecutors in the field. This is what the America Prosecutors Research Institute offers prosecutors now in the areas of DNA, child abuse, traffic prosecution and other areas, but they would have to have additional funding to provide this in the area of cybercrime.

Courts are nowhere close to dealing with cybercrime. Does the right to confront witnesses means that the witness must physically sit in the courtroom or can they testify by internet hook-up? This is especially relevant if we are going to prosecute an on-line theft scheme with hundreds of victims in dozens of locations. There are problems of venue, of twisting old laws to fit new crimes and fashioning a sentence for an 18 year-old whose computer virus has caused a million dollars in system damages.

4. Often it is a matter of resources in another State. It is not that the investigators resent helping you, it is just that they have a full caseload and no extra bodies to drop everything to go apply for a warrant on an ISP or a bad guy's computers, and then get a search team that knows what it is doing, and seize, inventory and store evidence and transmit it to another jurisdiction. Nor does the local prosecutor have the expertise to compel an ISP to comply with a court order or prevent disclosure to the customer.

The other problem of jurisdiction may be that of serving a subpoena or a court order issued by a Maryland court, for example, on a corporation in Virginia. The corporation does not have to accept a subpoena or order from a court that does not have physical jurisdiction over it. There are States that have made exceptions by requiring that ISP's who do business in that State must have a resident agent there to accept warrants, subpoenas and orders.

This problem could be solved in some respects by having a Federal long arm statute that authorized ISP's to give full faith and credit to warrants, subpoenas and orders issued in any State that appear valid on their face.

5. Distance. The prosecutor is unable to bring witnesses from other States to appear in court for internet theft cases, especially where each victim is only out $50 or less and there are dozens of victims. The prosecutor is unable to bring police investigators, records custodians or forensic experts from out of their jurisdictions or to introduce the evidence without these witnesses.

Lack of knowledge of both computers, the internet and the laws governing them at the State and federal levels. Lack of resources to transport witnesses, to present evidence in the courts and litigate complex issues. Keep in mind that half of the county prosecutors in the U.S. operate with a staff of less than 5 attorneys.

6. No. I believe that the internet could furnish a hotline to e-mail questions to a resource attorney that I referred to earlier, and as a website for new laws and developments but I think that the need to deal with local statutes and court procedures that differ from State to State would make one size fits all internet training impracticable. There is also no sense in teaching a standard procedure that has not been adopted or funded by individual jurisdictions.

7 I am going to answer a and b together. If Congress is going to provide the funding for regional labs, then Congress can mandate the standards and procedures that they have to adopt to qualify for the funding. Those standards and procedures can be the forensic industry best. If there is only regional labs funding for agencies that cooperate and share, then they will cooperate and share. These labs would end up being the "only game in town" and I believe many agencies would jump at such a resource. I urge you to ask the folks at the San Diego lab for their opinion.

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

July 18, 2001

The Honorable Lamar S. Smith
Chairman
Subcommittee on Crime
Committee on the Judiciary
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

Enclosed please find responses to post-hearing questions submitted to Mr. Michael Chertoff, Assistant Attorney General, Criminal Division, following a hearing before the Subcommittee on June 12, 2001, at which Mr. Chertoff testified. We hope that you will find the information helpful, and that you will not hesitate to call upon us if we may be of additional assistance in connection with this or any other matter.

Sincerely,

Daniel J. Bryant
Assistant Attorney General

Enclosures

cc: The Honorable Bobby Scott
Ranking Minority Member

ANSWERS TO POST HEARING QUESTIONS FOR
JUNE 12, 2001 HEARING ON FIGHTING CYBERCRIME
HEARING 2 OF 3: EFFORTS BY FEDERAL LAW ENFORCEMENT OFFICIALS

RESPONSES OF MICHAEL CHERTOFF
ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION
U.S. DEPARTMENT OF JUSTICE

1. The 1986 pen register and trap and trace statute, 18 U.S.C. §§3121-3127 established procedures for law enforcement authorities to collect the non-content information (i.e.,the source-but not the content associated with a communication.) Pen registers are devices that record the numbers dialed on a telephone line and trap and trace devices capture incoming electronic impulses that identify the originating number.

In the Clinton Administration's March 2000 report entitled "The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet," the Working Group reported that this statute was not adequate for trap and trace over the Internet. The working group provided the example that the statute refers to a device that is attached to a telephone line. The statute also is antiquated because it focuses specifically on telephone "numbers," and the tracing communications over the Internet may use other means to identify users' accounts. Additionally, the working group pointed out that the statute only allows a court to order communications carriers within its district to provide tracing information to law enforcement and as a result investigators have to apply for several court orders to trace a single communications these days. Do you agree or disagree with this conclusion? Please explain your answer.

A: The Department's experience investigating online crime suggests that the pen register/trap and trace statute, originally enacted in 1986, is in need of updating in two principal areas. First, there is a need to clarify that the statute does not apply only to traditional telephone communications, but also to newer communications technologies used to commit crimes. Second, changes in the telecommunications industry — as well as the emergence of new communications technologies — often require prosecutors to obtain multiple orders to trace a single communication, threatening investigations and needlessly wasting resources.

As discussed in the written testimony, the statute authorizes law enforcement to apply to a court for authorization to gather the telephone numbers dialed on a telephone line, or to collect the numbers of telephones used to dial a suspect's telephone. In the fifteen years since the statute was passed, new communications media, such as e-mail, have expanded dramatically. Criminals, too, employ the new methods of communication to commit a variety of crimes — from Internet fraud and identity theft to trafficking in narcotics or child pornography — and law enforcement investigators have had to adapt their investigative strategies accordingly. In the early stage of a case, those strategies often

require the identification of participants in a criminal scheme by identifiers such as email addresses.

In general, judges have recognized the obvious analogy between telephone numbers and identifiers used on other types of networks. Accordingly, courts have in appropriate cases issued pen/trap orders to collect such information as the "to" and "from" information of e-mails sent or received by a particular criminal's account. In one recent case, a pen/trap order on an e-mail account provided information critical to the arrest of accused murderer James ("Atomic Dog") Kopp, a Ten Most Wanted fugitive who had managed to evade authorities for four years.

These successes have not come without costs, however. Some Internet service providers have objected to such use of the statute, hampering (and even halting) investigations and causing needless expenditure of scarce prosecutorial resources to resolve these disputes. For that reason, the Department believes that the statute's applicability to non-telephonic forms of communication should be clarified, so as to remove doubt and enable investigators and prosecutors to combat crime committed using new technologies.

In addition, under present law, a court may only authorize the installation of a pen register or trap device "within the jurisdiction of the court." As a result, when one provider indicates that the source of a communication is a different carrier in another district, not only is a second order necessary, but it must be acquired by a prosecutor in that new district from a local judge – neither of whom has any other interest in the case. Indeed, in one case the Justice Department needed four separate orders to trace a hacker's communications. This duplicative process of obtaining a separate order for each link in the communications chain can thwart important investigations without any privacy benefits since the original court has already authorized the trace. Such duplication of effort only hinders investigations and benefits criminals.

2. In your written testimony you mention that the adequacy of penalties for certain computer crimes have been questioned. You state that prosecutors have expressed concern that the particular statutory approach for computing the minimum thresholds of damage in computer hacking cases may allow some significant criminals to go unpunished. Please explain what you mean and please address Mr. Davidson's concern that removing the minimum thresholds will make *de minimis* activity or online pranks serious federal crimes.

A: The Justice Department's experience in prosecuting computer crime suggests that the Congress should consider the adequacy of the current penalty scheme in two situations: where there may be serious harm but a low loss figure, and where there is a great deal of loss.

As to the low loss cases, the Department of Justice has encountered numerous instances where criminals have attempted to access or damage critical government and private-

sector systems that are used to provide critical infrastructure services, including telecommunications, transportation, and financial services. We were unable to prosecute several of these incidents because 18 U.S.C. §1030 generally requires evidence of damages in excess of $5,000. This is unfortunate as threats to these services, regardless of the dollar amount of damages, pose extreme risks to our infrastructure. When intruders gain unauthorized access to computers that hospitals use to store sensitive information and to treat patients, or that the military uses to defend the nation, federal prosecution of these individuals may be appropriate. These types of incidents are not merely *de minimis* activities or online pranks, but activities that threaten the day-to-day functioning of our society.

In addition, there is some question whether the penalties provisions of 18 U.S.C. § 1030 would reach a computer hacker who causes a large amount of damage to a network of computers if no individual computer sustains over $5,000 worth of damage. If section 1030 is not applicable in such a situation, then the Department's efforts to combat such crimes as denial of service attacks or the dissemination of viruses will be severely hampered. That is, an individual could cause tremendous financial damage to thousands of computers across the country but might not be punished because a single computer did not have $5,000 worth of damage. It would be useful to clarify that aggregation of damages is proper.

Another problem is that the Sentencing Guidelines require a minimum sentence of at least six months for violations of certain subsections of 18 U.S.C. §1030. In some instances, prosecutors have exercised their discretion and elected not to charge some defendants whose actions otherwise would qualify them for prosecution under that section, knowing that the result would be mandatory imprisonment. Congress may wish to consider whether requiring imprisonment for six months should be applied in more limited circumstances than allowed under existing law, and whether other punishments, such as reduced penalties and forfeiture of any instrumentalities or proceeds of the violation, might provide adequate punishment and deterrence.

3. What is the Department of Justice doing in response to the increase in denial-of-service attacks?

A: The Department takes all network crimes, including denial of service attacks, seriously and is doing everything in its power to identify those responsible for such crimes and bring them to justice. We have developed extensive investigatory and prosecutorial programs to cybercrime, whether it be intrusions, denial of service attacks, or the dissemination of malicious virus code.

For example, on the investigative side, we have the FBI's National Infrastructure Protection Center (NIPC) and specialized squads located in 16 field offices. (We also work with agents in the U.S. Customs Service, the Secret Service, NASA, the

Department of Defense, and others.) On the prosecutorial side, we have trained attorneys, both in Washington, D.C. and in the field, who are experts in the legal, technological, and practical challenges involved in investigating and prosecuting cybercrime. These prosecutors are guided by the Computer Crime and Intellectual Property Section, or CCIPS, which currently has 23 attorneys. In the field, the Department has Assistant United States Attorneys known as "Computer and Telecommunications Coordinators" (CTCs) in U.S. Attorneys' Offices around the country. Each CTC is given special training and equipment, and serves as the district's expert in computer crime cases. In addition, the Department regularly works with other international, federal, state, and local investigators and prosecutors to combat cybercrime. The importance of these domestic and international efforts was recently highlighted by our success in tracking down the perpetrator of the major distributed denial of service attacks launched against Yahoo!, Ebay, CNN and others in February 2000. CCIPS, working with numerous FBI and U.S. Attorneys Offices, tracked the hacker back to Canada. Canadian and U.S. law enforcement worked closely together to identify a Canadian juvenile with the computer moniker "mafaiboy" who has been charged and pled guilty to the denial of service attacks in Canada.

The Department is also working with the private sector to encourage the reporting of cybercrimes, as well as to encourage information sharing between the private sector and government. We recognize that combating cybercrime requires a two-fold approach. On one hand, we need to ensure that the private sector is aware of the immediate and most current threats to the nation's infrastructure and computers. On the other hand, we must strive to put those responsible for those threats behind bars where they cannot continue to improve upon their criminal techniques and release more sophisticated threats against our infrastructure. The Department is dedicated to balancing these efforts to ensure that we can both protect our systems and prevent them from being attacked in the future.

4. It's my understanding that one goal of the Department of Justice's Intellectual Property Enforcement Initiative is to vigorously enforce laws against "hard goods piracy." U.S. companies are losing billions of dollars each year on "copyright and trademark infringing items" shipped from such places as Asia and Latin America. Often these items are transshipped through U.S. ports, giving rise to U.S. investigative jurisdiction. Will you continue to support investigation and prosecution of these types of cases? Do you have any specific plans to review U.S. Customs seizures and investigations for consideration as criminal prosecutions?

A: The primary goal of the Department's Intellectual Property Enforcement Initiative (IP Initiative) is to promote the investigation and prosecution of all forms of intellectual property crime, whether committed online or involving "hard goods." The Department of Justice has and will continue to support the prosecution of such cases. The Department, on a regular basis, is in contact with the U.S. Customs Service to review their seizures and determine the potential for criminal prosecution. Interaction with Customs occurs most frequently through the U.S. Attorneys Offices in the cities and locations where the

seizures occur.

Additionally, the Department works closely with Customs agents on a number of IP issues, including as a full partner in the IP Initiative. The Computer Crime and Intellectual Property Section of the Criminal Division, which spearheads our IP efforts, has dedicated resources to ensure that the Department and all investigative agencies, including Customs, are working together in responding to criminal violations of intellectual property laws. Also, the Department supports the Intellectual Property Rights (IPR) Center in Washington, D.C., a joint FBI-Customs operation which facilitates the successful investigation and prosecution of IP crimes nationwide. The Department looks forward to continuing to a continued close working relationship with the Customs Service in the coming years.

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

August 6, 2001

Honorable Lamar Smith
Chairman
Subcommittee on Crime
House of Representatives
Washington, DC 20515-6216

Dear Mr. Chairman:

Thank you for allowing me to testify on June 12, 2001, before the Committee on the Judiciary, Subcommittee on Crime, concerning the oversight on fighting Cyber Crime. Cyber Crime, as you are well aware, is presenting many sensitive issues that must be addressed by law enforcement.

Enclosed, please find my responses to the post hearing questions. I hope my testimony and answers to your follow-up questions will prove helpful in deliberating these issues.

Thank you again for allowing me to speak to you regarding this very important issue.

Sincerely,

Thomas T. Kubic
Principal Deputy Assistant Director
Criminal Investigative Division

Enclosure

POST HEARING QUESTIONS FOR
JUNE 12, 2001 HEARING ON FIGHTING CYBER CRIME - HEARING 2 OF 3:
EFFORTS BY FEDERAL LAW ENFORCEMENT OFFICIALS

Questions for Mr. Kubic, Deputy Assistant Director, FBI

1. **In your testimony, you stated that fraud committed over the Internet is the same type of white collar fraud that the FBI has traditionally investigated but poses additional concerns and challenges. You state that because of the accessability of such an immense audience as the Internet provides and the anonymity of the subject, a different approach must be taken. Please describe that different approach.**

A different approach must be taken related to fraud that is committed utilizing the Internet because of several factors, to include a high degree of anonymity available to subjects and the immense audience provided by the Internet. Because of the speed and potential magnitude in which a fraudster can effect a crime, often law enforcement must initiate a case prior to determining the subjects identity and the best venue for prosecution. Most often, only after a case is initiated and subpoenas are issued, can the subjects location and true identity be determined. This can only be accomplished with the assistance provided by victims, and most importantly Internet Service Providers (ISP's). Quite often the information being provided by the ISP's needs to be interpreted for the investigator by staff of the ISP or an investigator with specialized training in hi-tech matters. Once the subjects location is determined, an investigator who initiated the case most often must refer the matter to another jurisdiction. This is due to the fact that the investigation may have to be referred to the best venue for prosecution.

As a result, agencies involved in Internet related investigations must be prepared at the outset of an investigation that any work accomplished prior to the identification of a subject may ultimately be relayed to another agency for prosecution. In particular for State and Local Law Enforcement agencies with defined geographical jurisdiction, this may be a limiting factor when determining whether or not to initiate an investigation.

2. **You testified that victims of Internet fraud have been unsure of how or where to report their experiences and law enforcement agencies have received complaints in a piecemeal fashion so that the complaint does not advance to an investigation. You also state that venue is a problem as it is difficult to identify the location of a web site or the origin of an E-mail. How would the FBI address these problems?**

In a traditional white collar crime investigation the victim contacts law enforcement authorities about a subject who most often has a known location. An investigation is usually initiated once law enforcement authorities determine they have jurisdiction. However, many victims of Internet crime can not identify the subject other than to provide an e-mail or web site address. Additionally, cases involving multiple victims often report different identifying data, such as an email addresses, which may be associated with the same individual. Single complaints being filed independently to different law enforcement agencies throughout the country makes it almost impossible to determine the true scope of a fraud.

Unlike existing complaint centers, the IFCC not only compiles complaints, but they refer each valid complaint to numerous federal, state, and local agencies. The IFCC staff processes incoming complaints and forwards them to an average of three to four law enforcement agencies. In its first year of operation, the IFCC received over 30,000 valid Internet fraud complaints, which spawned hundreds of criminal investigations throughout the country. The FBI staff then began to use the matured data base to identify additional cases involving multiple victims and subjects perpetrating numerous which were previously thought to be unrelated. This analysis initiated the investigative phase of the Center's operation. Utilizing this process, the IFCC staff drafted over 545 Internet Investigative Reports and forwarded them to 51 of 56 FBI Field Offices and over 1,500 state and local law enforcement agencies. The IFCC also referred 41 cases encompassing over 200 complaints to international law enforcement agencies. The IFCC monitors and coordinate's these international cases.

The IFCC also initiated Operation Cyber Loss, which involved 26 FBI Field Offices, the U.S. Postal Service, the Internal Revenue Service, the U.S. Customs Service, and numerous state and local law enforcement entities. The Internet fraud schemes exposed as part of the initiatives represented over 56,000 victims nationwide, suffering cumulative losses in excess of $117,000,000. Approximately 90 subjects have been charged in Operation Cyber Loss for wire fraud, mail fraud, conspiracy to commit fraud, money laundering, bank fraud, and intellectual property rights violations.

3. **Describe what the National Infrastructure Protection Center does with regard to cyber crime.**

The mission of the National Infrastructure Protection Center (NIPC) (in priority order) is to detect, deter, assess, warn (users), respond to, and investigate unlawful acts involving computer and information technologies and unlawful physical and cyber acts that threaten or target our critical infrastructures. The NIPC closely coordinates its work with the Computer Analysis Response Teams in the FBI Laboratory Division, who analyze computer media for evidence, and with the Internet Fraud Complaint Center, which accepts complaints from consumers involving fraud over the Internet. In carrying out its mission, the NIPC pursues three sets of activities with regard to computer intrusions: prevention, detection, and response.

Prevention:

The NIPC's role in preventing cyber intrusions is not to provide advice on what hardware or software to use or to act as a systems administrator. Rather the Center's role is to provide information about threats, ongoing incidents, and exploited vulnerabilities so that government and private sector system administrators can take the appropriate protective measures. The NIPC has a variety of products to inform the private sector and other domestic and international government agencies of the threat, including: alerts, advisories, and assessments; biweekly *CyberNotes*; monthly *Highlights*; and topical electronic reports. These products are designed for tiered distribution to both government and private sector entities consistent with applicable law and the need to protect intelligence sources and methods, and law enforcement investigations.

The NIPC has elements responsible for both analysis and warning. What makes the NIPC unique is that it has access to all-source intelligence from law enforcement, the intelligence community, private sector, international arena, and open sources. No other entity has this range of information. Complete and timely reporting of incidents from private industry and government agencies allows NIPC analysts to make the linkages between government intrusions and private sector activity. NIPC is currently working on an integrated database to allow us to more quickly make the linkages among seemingly disparate intrusions. This database will leverage both the unique information available to the NIPC through FBI investigations and

information available from the intelligence community and open sources. Having these analytic functions at the NIPC is a central element of its ability to carry out its preventive mission.

The NIPC's InfraGard initiative expands direct contacts with the private sector infrastructure owners and operators and shares information about cyber intrusions and exploited vulnerabilities through the formation of local InfraGard chapters within the jurisdiction of each of the 56 FBI Field Offices. This is critical to infrastructure protection, since private industry owns most of the infrastructures. All 56 FBI field offices have InfraGard chapters. There are currently over 1300 InfraGard members.

The NIPC is also working with the Information Sharing and Analysis Centers established under the auspices of PDD-63. For example, the North American Electric Reliability Council (NERC) serves as the electric power ISAC. The NIPC has developed a program with the NERC to develop an Indications and Warning System for physical and cyber attacks. Under the program, electric utility companies and other power entities transmit incident reports to the NIPC. These reports are analyzed and assessed to determine whether an NIPC alert, advisory, or assessment is warranted to the electric utility community. Electric power participants in the pilot program have stated that the information and analysis provided by the NIPC back to the power companies make this program especially worthwhile. NERC has recently decided to expand this initiative nationwide.

Detection:

Given the ubiquitous vulnerabilities in existing Commercial Off-the-Shelf (COTS) software, intrusions into critical systems are inevitable for the foreseeable future. Thus detection of these intrusions is critical if the U.S. Government and critical infrastructure owners and operators are going to be able to respond. To improve our detection capabilities, the NIPC first needs to ensure that it is fully collecting, sharing, and analyzing all extant information from all relevant sources. It is often the case that intrusions can be discerned simply by collecting bits of information from various sources;

conversely, if these pieces of information are not collected for analysis, intrusions might not be detected at all. Thus the NIPC's role in collecting information from all sources and performing analysis in itself serves the role of detection.

In some cases, in response to victims' reports, the NIPC has sponsored the development of tools to detect malicious software code. For example, in December 1999, in anticipation of possible Y2K related malicious conduct, the NIPC posted a detection tool on its web site that allowed systems administrators to detect the presence of certain Distributed Denial of Service (DDoS) tools on their networks. In these cases, hackers plant tools such as Trinoo, Tribal Flood Net (TFN), TFN2K, or Stacheldraht (German for barbed wire) on a number of unwitting victim systems. Then when the hacker sends the command, the victim systems in turn begin sending messages against a target system. The target system is overwhelmed with the traffic and is unable to function. Users trying to access that system are denied its services. The NIPC's detection tools were downloaded thousands of times and have no doubt prevented many DDoS attacks.

Regarding warning, if NIPC determines that an intrusion is imminent or underway, the NIPC Watch is responsible for formulating assessments, advisories, and alerts, and quickly disseminating them. The substance of those products will come from analytical work done by NIPC analysts. If we determine an attack is underway, we can notify both private sector and government entities using an array of mechanisms so they can take protective steps. In some cases these warning products can prevent a wider attack; in other cases warnings can mitigate an attack already underway. Finally, these notices can prevent attacks from ever happening in the first place. For example, the NIPC released an advisory on March 30, 2001 regarding the "Lion Internet Worm," which is a DDoS tool targeting Unix-based systems. Based on all-source information and analysis, the NIPC alerted systems administrators how to look for this compromise of their system and what specific steps to take to remove the tools if they are found. This alert was issued after consultation with FedCIRC, JTF-CND, a private sector ISAC, and other infrastructure partners.

Response:

A vital part of the NIPC's mission is to investigate computer intrusions. Because the Internet by its nature embodies a degree of anonymity, our government's proper response to an attack first requires significant investigative steps. Investigators typically need a full range of criminal and/or national security authorities to determine who launched the attack. Under our system the legal authorities for conducting investigations within the United States include: the Computer Fraud and Abuse Act, the Economic Espionage Statute, the Electronic Communications Privacy Act, the Foreign Intelligence Surveillance Act, as well as the relevant executive orders delineating the responsibilities of the intelligence community. Thus the FBI can apply for court orders to get subscriber information from Internet Service Providers, and monitor communications under the Electronic Communications Privacy Act or under the Foreign Intelligence Surveillance Act, depending on the facts of the case, as they are known at the time the order is requested. The FBI has designated the NIPC to act as the program manager for all of its computer intrusion investigations, and the NIPC has made enormous strides in developing this critical nationwide program.

4. What is the mission and role of the Internet Fraud Complaint Center (IFCC)?

The IFCC has developed and implemented a national strategy to identify and track fraud, analyze Internet crime trends, link related Internet complaints, develop investigative packets, and forward information to the appropriate investigative agencies.

The center is part of a cyber community watch in which the Internet community, composed of users, providers, and merchants, identify potential criminal activity over the Internet then report the activity to the IFCC.

a. How does the FBI work with the private sector in running the center?

The private sector does not run the IFCC. However, prior to the opening of the IFCC, FBI personnel sought advice from private industry to better address the needs of these crime victims. The private sector enhanced the electronic complaint process and worked within their own particular industries to ferret out fraud.

The FBI is also working with the private sector to create a working group-type network to receive information from the private sector, discuss pertinent information technology issues and goals, recommend legislative solutions, and exchange ideas to address problems and find solutions. The IFCC is working with the private sector to develop a new information technology system to enable the simultaneous referral of multiple complaints from e-commerce companies.

b. You mention the creation of a national strategic plan to address Internet fraud. When will that plan be done and how does it address coordination and cooperation among federal, state, and local law enforcement, and the private sector including academia?

A program plan to combat Internet fraud was developed and implemented. It is part of the FBI's overall Internet Fraud Strategy. This plan is complementary with the FBI National Strategic Plan.

5. With regard to malicious intrusions, how do you determine whether you are dealing with a terrorist act or another form of cyber crime and what are the steps you take after that determination?

In the cyber world, determining what is happening is difficult at the early stages. An event could be a system probe to find vulnerabilities or entry points, an intrusion to steal data or plant sniffers or malicious code, an act of teenage vandalism, an attack to disrupt or deny service, or even an act of war. The crime scene itself is totally different from the physical world in that it is dynamic--it grows, contracts, and can change shape. Further, the tools used to perpetrate a major infrastructure attack can be the same ones used for other cyber intrusions (simple hacking, foreign intelligence gathering, organized crime activity to steal property, data, etc...), making identification more difficult. Determining that an event is even occurring thus can often be difficult in the cyber world, and usually a determination cannot be made without a thorough investigation. In the physical world one can see instantly if a building has been bombed or an airliner brought down. In the cyber world, an intrusion may go undetected for some time.

Identification of the perpetrators and their objectives during an event is critical especially in the initial stages. The perpetrators could be criminal hackers, teenagers, electronic protestors, terrorists, or foreign intelligence services. In order to attribute an attack, the NIPC coordinates an investigation that gathers information

from within the United Sates using either criminal investigative or foreign counter-intelligence authorities, depending on the circumstances. We also rely on the assistance of other nations when appropriate. Obtaining reliable information is necessary not only to identify the perpetrator but also to determine the size and nature of the intrusion: how many systems are affected, what techniques are being used, and what is the purpose of the intrusions--disruption, economic espionage, theft of money, etc...

Relevant information could come from existing criminal investigations or other contacts at the FBI Field Office level. It could come from the U.S. Intelligence Community, other U.S. Government agency information, through private sector contacts, the media, other open sources, or foreign law enforcement contacts. The NIPC's role is to coordinate, collect, analyze, and disseminate this information. Indeed this is one of the principal reasons the NIPC was created.

In the event of a national-level set of intrusions into significant systems, the NIPC will form a Cyber Crisis Action Team (C-CAT) to coordinate response activities and use the facilities of the FBI's Strategic Information and Operations Center (SIOC). The team will have expert investigators, computer scientists, analysts, watch standers, and other U.S. government agency representatives. Part of the U.S. government team might be physically located at FBI.

Headquarters and part of the team may be just electronically connected. The C-CAT will immediately contact field offices responsible for the jurisdictions where the attacks are occurring and where the attacks may be originating. The C-CAT will continually assess the situation and support/coordinate investigative activities, issue updated warnings, as necessary, to all those affected by or responding to the crisis. The C-CAT will then coordinate the investigative effort to discern the scope of the attack, the technology being used, and the possible source and purpose of the attack.

Once the above are determined, the NIPC will work with other elements of the executive branch to formulate a response, which could range from criminal prosecution through diplomatic or even military action, depending on circumstances.

6. **At the first cyber-hearing on May 24th, all of the witnesses recommended the creation of more regional computer forensic laboratories. Currently, as I understand, there is one in Dallas, Texas**

and one in San Diego, California.

a. Have any of you participated or are you familiar with these regional laboratories?

The FBI has participated in two pilot Regional Computer Forensic Labs (RCFL's), 1) the San Diego Regional Computer Forensic Lab, and , 2) the North Texas Regional Computer Lab. The FBI will participate in another similar lab which is still being finalized in Columbia, South Carolina.

Consistent with the FBI Laboratory's mission to provide forensic services to state and local agencies, the FBI has provided personnel resources, training, and computer forensics equipment and supplies to support the RCFLs in San Diego and Dallas. The respective FBI field offices dedicated Computer Analysis Recovery Team (CART) field examiners, space and management in support of these facilities.

Much has been learned from these two pilot programs that will facilitate the development of any future RCFL's. Among the lessons learned was that there needs to be strong leadership and a solid legal foundation for each RCFL.

b. Would you agree or disagree with the proposal?

The Code of Federal Regulations vests within the FBI Laboratory a unique authority. Pursuant to 28 C.F.R. §0.85, the FBI Laboratory may assist, at no cost, any duly constituted law enforcement agency (including State and local agencies) seeking assistance with the forensic examination of digital evidence regardless of whether such evidence was relevant to a federal crime.

Title V (5 U.S.C. §3374) provides for the assignment of state or local government employees to the FBI (and other federal agencies) on a detail basis. During the period of assignment, a state or local employee on detail to the FBI is deemed an employee of the agency for the purposes of the Federal Tort Claims Act and any other Federal tort liability statute and therefore receives the same liability protections of federal employees.

A combination of these two provisions will allow the FBI to place employees of state and local law enforcement agencies on assignment within the FBI Laboratory and thus allow them to take advantage of the Laboratory's unique status under Title 28 of the C.F.R.

Because it is in the interests of the FBI and the United

States to promote and facilitate the creation, development and propagation of uniform, scientifically-sound policies, procedures, practices, protocols, guidelines and techniques relating to the forensic examination of digital evidence, the FBI Laboratory supports the requirement for a number of these joint RCFL's. As the recognized leader in computer forensics, we believe that the best way to accomplish this is to provide directed funding to the FBI for the development of additional RCFL's.

DEPARTMENT OF THE TREASURY
UNITED STATES SECRET SERVICE

The Honorable Lamar Smith
Chairman
Subcommittee on Crime
House Committee on the Judiciary
U.S. House of Representatives
Washington, D.C. 20510

Dear Mr. Chairman:

Thank you for your recent correspondence inviting the Secret Service to respond to several follow-up questions from the June 12, 2001, hearing on federal efforts to combat cyber crime.

Enclosed, please find a complete set of responses from Mr. James A. Savage, Jr., Deputy Special Agent in Charge of the Secret Service's Financial Crimes Division. I hope this information is helpful to the subcommittee, and, as always, the Secret Service would be delighted to provide any additional information the subcommittee may require.

Thank you again for the opportunity to testify on this important issue. If I can be further assistance to you on this or any other issue, please do not hesitate to contact me at (202) 406-5676.

Sincerely,

Paul D. Irving
Deputy Assistant Director

Post-Hearing Questions for
Mr. James A. Savage, Jr.
Deputy Special Agent in Charge -- Financial Crimes Division
United States Secret Service

Hearing on June 12, 2001
Efforts by Federal Law Enforcement Officials to Combat Cyber Crime
Subcommittee on Crime
House Committee on the Judiciary

1. **You testified that the New York Electronic Crimes Task Force is a model for the partnership approach with law enforcement and private industry. Has the Secret Service established any similar task forces in the country? If not, do you plan to establish any more?**

The Secret Service does view the New York Electronic Crimes Task Force (NYECTF) as the model for the partnership approach that we hope to employ in additional venues around the country. In June of this year, a new electronic crimes task force was established in Washington, D.C. based upon the NYECTF model.

The primary obstacle to establishing such task forces is funding. Not only do office space, furniture, computers, office equipment and supplies, and telecommunications services all need to be procured, but because of the specialized nature of electronic crimes investigations, steps need to be taken to provide additional training for task force members. For such task forces to be fully successful:

- Electronic Crimes Special Agent Program (ECSAP) training and equipment is required for at least two of the Secret Service special agents assigned to each task force, and in-service training and equipment updates are needed for these agents on an annual basis after the completion of their initial training,

- Secret Service-sponsored training is needed for federal, state and local task force counterparts to improve liaison, impart knowledge of the Secret Service mission, and ensure greater cooperation in task force operations, and

- Annual training on specialized investigative techniques and task force operations is needed for Secret Service special agents and criminal research specialists assigned to the task forces, and for selected non-Secret Service task members, to keep them abreast of new developments in the rapidly changing arena of electronic crime.

Such training demonstrates the commitment of the Secret Service to the task force concept, thereby establishing the new relationships, and further improving the existing ones, that are

essential to the success of such an initiative. By providing investigative training to the Secret Service personnel assigned to the task forces, the Secret Service can increase their efficiency and effectiveness, and maximize the return on its investment.

Accordingly, the Secret Service will be forwarding to the Department of the Treasury a request to expand these task forces to at least 7 other offices nationwide. These cities will be selected based upon a variety of factors, including:

- The presence of financial industry, information technology, and government entities that are the most frequent targets of electronic crimes,
- The perceived need for such a task force as estimated by Financial Crimes Division and the affected field offices,
- Industry figures concerning computer intrusions and other high tech crimes, and
- The willingness of law enforcement agencies and private industry in these cities to actively participate in such an initiative.

If this initaitive is funded, the Secret Service, through the strategic placement of these specialized task forces, would work in conjunction with other federal, state and local law enforcement entities, as well as private sector counterparts, to decrease the incidence of electronic and financial crimes in the targeted cities through the arrest and prosecution of individuals and organized criminal enterprises involved in the commission of financial crimes.

2. Please explain what benefits the Secret Service has experienced from information sharing with other law enforcement, the private sector, and academia.

The Secret Service has always worked closely with other law enforcement agencies in the investigation and prevention of electronic and financial crimes. The Secret Service has long recognized the value in sharing information during the course of our investigations with both those in the private sector and academia who are devoting substantial resources to protecting their networks and researching new solutions. It is not uncommon for us to share case-specific information derived from our criminal investigations after taking appropriate steps to protect privacy concerns and ensure that there are no conflicts with prosecutorial issues. Our willingness to share information with these entities has enabled us to develop and maintain avenues for obtaining:

- Full cooperation that leads to successful joint operations/investigations;
- Prompt and direct notification regarding crimes within our jurisdiction;
- Case specific assistance regarding unusually complex systems and devices, and previously unknown or deceptive computer intrusion techniques or utilities;
- Training and mentoring from talented computer security professionals and experts in other highly technical fields;
- General criminal intelligence information, and

- Information regarding new technologies and their possible applications to criminal activities, Because of the rapid pace of change in computer and telecommunications systems, we could not successfully investigate complex electronic cases without the direct support of our private sector counterparts.

3. You testified that in one investigation the case agent actually specified in the affidavit of the federal search warrant that representatives of the victim business be allowed to accompany federal agents in the search of the target residence to provide technical assistance. How do you protect legitimate trade secrets from competing businesses in situations like this?

The example referred to in my testimony involved a situation where the private sector representatives were needed to provide on-site technical assistance regarding certain aspects of their own products. Furthermore, such technical assistance would only be requested from a representative of a victim business -- never from a competitor. In cases involving multiple victims, private sector participants would not be privy to all the information obtained through the service of the warrant, they would only examine or analyze items related to their own company, and they would not examine an item unless requested to do so by the Secret Service.

Additionally, the New York Electronic Crimes Task Force model places the obligation on all task force members, whether private, public, or academic, to maintain a policy of non-disclosure regarding all proprietary information. In such a situation, it is in everyone's self-interest to operate in an atmosphere of trust and confidentiality, and unless all participants agree not to misuse the privileged information, this environment cannot exist. By carefully promoting the trust and confidence of task force partners with responsible actions, the protection of information is maintained and ensured.

Such an approach is clearly non-traditional, and represents a paradigm shift. But the speed at which new technologies are being developed obligates law enforcement to depend on the developers of these technologies to provide the technical expertise needed to assist in the successful investigation of new types of electronic crimes.

4. In many of your examples in the testimony, it appears the criminal was actually a disgruntled former employee. How often is this the case?

The Secret Service does not maintain statistics concerning "insider involvement" computer intrusion or denial-of-service investigations, but our anecdotal evidence and industry statistics indicate that disgruntled former employees are involved in a significant percentage of such cases, and are responsible for the most financially devastating losses.

This is not particularly surprising, given that such individuals usually have insider information concerning network system vulnerabilities, and in their mind, have a justifiable motive. As with any type of crime, the confluence of motive and opportunity often lead to criminal behavior.

As a result, businesses need to be cognizant of the risks posed by employees in technical positions who separate from the company under unpleasant circumstances, and take appropriate network security countermeasures.

5. How do you work with the FBI on child pornography cases?

The Secret Service does not have jurisdiction to investigate child pornography violations, although we do provide computer forensics assistance to other law enforcement agencies upon request. Because the FBI has its own computer forensics program, they have not had occasion to request our assistance in these types of cases.

Over the past three years, Secret Service ECSAP agents completed 2,122 examinations on computer and telecommunications equipment. Although the Secret Service did not track the number of exams done for other law enforcement agencies during this period, it is estimated that some 10-15 percent of these examinations were in this category. Many of these were conducted not because the underlying case was of interest to the Secret Service (often they involved violations such as child pornography and murder), but because the requesting agency did not have the resources to complete the examination itself. Another estimated 30-40 percent involved examinations of equipment that was seized during a task force or other joint investigation.

6. You mentioned an interactive, computer-based training program to train officers to conduct electronic crime investigations. Is this an on-line program? Some have suggested that on-line training programs provide better access at a lesser cost to the government. Do you agree?

This training program, Forward Edge, is not an on-line program; it is CD-ROM based. Forward Edge is an interactive training program based on virtual reality situations, and as a result it incorporates a technology that requires considerable storage space and bandwidth. These requirements would make it difficult to deploy over an on-line connection because of the high connection speed that would be required (a dial-up connection would not be adequate).

The Secret Service does agree that on-line training is extremely cost effective, and as a result we are pursuing other types of on-line training when the type of training and the technologies involved permit us to do so.

7. At the first cyber-hearing on May 24th, all of the witnesses recommended the creation of more regional computer forensic laboratories. Currently, as I understand, there is one in Dallas, Texas, and one in San Diego, California.

a. Have any of you participated or are you familiar with these regional laboratories?
b. Would you agree or disagree with this proposal?

The Secret Service is familiar with the Regional Computer Forensic Laboratory (RCFL) concept, and we do maintain liaison with the existing labs mentioned above. The Secret Service does recognize that the RCFLs are an excellent vehicle for providing a minimum level of services to agencies without computer forensic capabilities.

While our Electronic Crimes Special Agent Program (ECSAP) is different from the RCFLs, we do not necessarily view the two as being in competition with one another. Rather, each brings value to investigation of electronic crimes.

The concerns that the Secret Service has concerning the implementation of RCFLs can be summarized as follows:

- Based upon previous testimony from the FBI, the existing RCFLs already have a significant backlog of pending cases.

- Because the methodology of prioritizing cases is not yet fully developed, there seems to be some question as to whether participating agencies could get exams completed quickly when they feel they have a need to do so, or are requested to do so by a prosecutor.

- Typically financial crimes cases, our core jurisdiction, are given a low priority by laboratories that are required to handle a variety of cases.

- The RCFLs function like a traditional laboratory in that the electronic evidence needs to be submitted to them for forensic examination and analysis. However, recent legal decisions have been limiting the amount of time a computer system can be held as evidence. Some search warrants only allow for an electronic image of a system's hard drive to be taken, rather than for the seizure of the machine itself. Yet the RCFLs are not primarily geared towards providing assistance to participating agencies in the seizure of electronic evidence.

- The RCFLs will use a combination of civilian technicians and criminal investigators to complete examinations. Although civilian examiners are more than capable of completing such examinations, they may not have the investigative experience necessary to allow them to discern what small portion of the vast amount of information contained in the electronic evidence under examination has significant evidentiary value.

- The RCFLs do not encourage private sector involvement, which could complicate efforts to complete examinations on certain new technologies and proprietary devices.

In contrast, ECSAP agents respond to crime and search scenes on short notice, and we have an excellent record of completing high priority exams in very short periods of time. ECSAP also utilizes experienced criminal investigators who have an expertise in the forensic examination and analysis of electronic evidence, and partners with private sector entities in overcoming the myriad obstacles that are frequently encountered in the investigation and prosecution of electronic crimes cases.

Let me be clear in saying that the Secret Service supports additional resources to combat electronic crimes, but believes that the use of such facilities or resources should be voluntary and not mandatory, nor should it be a prerequisite for federal prosecution.

Post Hearing Questions:
June 14, 2001 Hearing on Fighting Cyber Crime - Hearing 3 of 3:
Concerns of Private Industry

Responses to the following questions for Harris Miller, President - ITAA

1. *In your written testimony you state that cyber crime places the digital economy at risk. How serious is that risk?*

Response: The risk is significant and continues to grow. The Computer Security Institute's most recent survey reported nearly $400 million in losses by U.S. corporations to cyber-crime last year. That number is a very conservative estimate and doesn't account for break-ins and losses that were never reported. As the Internet becomes more pervasive and as more and more businesses put their operations on-line, the impact of cyber-crime on our economy -- and the global economy -- will continue to increase. Also, Cyber threats such as the ILOVEYOU virus and the Code Red Worm cost businesses billions of dollars in damage, productivity and revenue loss.

2. *In your testimony, you site some interesting statistics. You refer to an ITAA nationwide public opinion poll of 1000 Americans released last year that found that 67 percent are concerned or feel threatened by cyber-crime. That poll also found that 62 percent do not believe enough is being done to protect Internet consumers against cyber-crime. Additionally, 65 percent believe that on-line criminals have less of a chance of being caught than other criminals. Do you believe that the public's perception is accurate?*

Response: I think that there continues to be significant concern in the public about cyber-crime, and rightly so. High profile cyber threats such as the ILOVEYOU virus and the Code Red Worm certainly increase the amount of attention by users on the cyber crime issue and hopefully, also increase the number of steps that users take to enhance their information security practices. The technology is available to protect users' systems, but the vulnerabilities usually come from the "people and process" part of the equation. Our hope is that as users become more aware of information security, they will practice sound cyber hygiene.

While it's very difficult to track cyber attacks to their source, advancements in technology -- and improved cooperation with law enforcement through the FBI's InfraGuard program and other mechanisms -- is bearing fruit.

3. *You stated that organizations must be willing to invest in the development of comprehensive security procedures and to educate employees -- continuously. Are you members willing? Have you seen a big investment on their part?*

Response: Yes, our members are willing and many corporations -- big and small -- are making substantial investments in information security and in educating and training their employees to practice good cyber-hygiene and to create a larger pool of skilled

information security workers. These kinds of investments are increasing, but it's still not enough. Until information security is dealt with at the Board level and by senior management -- again in companies big and small -- the issue will not receive the needed attention and investment within the corporate structure. By the way, this process also applies to government at all levels. Until government leaders recognize this as a key issue that must be dealt with through both education and financial investments in technology and management processes, we should expect more reports of vulnerable systems by the GAO.

4. *In your testimony, you state that organizations must be prepared to cooperate with law enforcement.*
   a) *What do you believe are the consequences if organizations fail to cooperate?*
   b) *How can we get around companies concerns about disruptions to operations and the potential damage to their reputations by working with law enforcement?*
   c) *How do trade associations and groups like the Partnership for Critical Infrastructure Security help?*

Response: a) We need to develop relationships between law enforcement and the private sector that are built on trust and meaningful cooperation. That won't happen overnight. Improved information sharing between government and industry will be a step forward. b) Companies who participate in programs such as InfraGuard will become more comfortable in working with law enforcement. Once legal obstacles to information sharing between industry and government are overcome, companies could become more willing to share sensitive information with law enforcement and other federal agencies. c) ITAA, which has played a leading role in the information security area for a number of years, will continue to work with the IT industry and government to create and sustain meaningful partnerships and relationships. ITAA was instrumental in the development of the IT-ISAC (Information Sharing and Analysis Center) -- which is now becoming operational -- and was the leading trade association working behind the scenes to mobilize the industry-government coalition that responded to the recent Code Red Worm threat. The Partnership for Critical Infrastructure Security (PCIS) has the important role of helping to build cross-sector initiatives that promote and assure reliable provisions of critical infrastructure services in the face of emerging risks to economic and national security, including cyber-crime.

5. *Why is information sharing so important to the efforts against cyber-crime?*
   a) *Why is the Freedom of Information Act a barrier to information sharing?*
   b) *Some are concerned that information sharing between business for cyber security might violate anti-trust laws. Your written testimony seems to allay some of these concerns. Please describe in detail how such violations can be avoided when sharing information to combat cyber-crime?*
   c) *What is the purpose of the new IT-ISAC? Does this violate anti-trust laws?*

Response: a) Companies are concerned that information voluntarily shared with the government that reports on or concerns corporate security may be mistakenly subjected to FOIA. They are also concerned that lead government agencies may not be able to effectively control the use or dissemination of sensitive information because of similar legal requirements. Unfiltered, unmediated information may be misinterpreted by the public and undermine public confidence in the country's critical infrastructures. Also, business competitors and others may use shared information to the detriment of a reporting company, or as the basis for litigation. Any and all of these possibilities are reasons why the current flow of voluntary data is minimal. ITAA supports the clarification, not the abrogation of the Freedom of Information Act. The legislative proposals we support give our companies the unambiguous confirmation that their communications intended to aid in a joint defense from a common critical infrastructure protection threat are protected. b) Businesses need protection from unnecessary restrictions placed by federal and state antitrust laws on critical information sharing that would inhibit identification of R&D needs or the identification and mitigation of vulnerabilities. c) Major information technology companies joined together to form the IT-ISAC to report and exchange information concerning electronic incidents, threats, attacks, vulnerabilities, solutions and countermeasures, best security practices and other protective measures. The IT-ISAC enables the high tech industry to: 1) share state-of-the-art Internet and formation security measures, 2) spot potential threats to the Internet faster, and 3) respond rapidly when incidents occur.

There is uncertainty about whether existing law may expose companies and industries that voluntarily share sensitive information with the federal government to unintended and potentially harmful consequences. This uncertainty has a chilling effect on the growth of all information sharing organizations and the quality and quantity of information that they are able to gather and share with the federal government. ITAA is strongly in favor of removing disincentives to information sharing and that is why we support current legislation to address these issues.

6. *You expressed concerns about the Council of Europe draft Convention on Cyber-Crime. While this is a treaty and obviously a Senate ratification issue, would you please describe your concerns?*

Response: The Council of Europe Cybercrime Convention has improved in many respects through the efforts of the U.S. delegation. We were disappointed to learn that several changes of critical importance to us industry, privacy groups and noncommercial interests were not adopted in the final version of the convention. For example, the Convention does not address, including data retention and surveillance technology mandates, lack of reimbursement for compliance with surveillance mandates, lack of standard privacy protections for law enforcement requests, and potential liability for complying with requests. Therefore, we are concerned that implementation of the Convention will produce a patchwork of costly and inconsistent requirements worldwide that create significant market access barriers for communications companies, and undermine user privacy.

One important area of particular concern in implementation of the treaty is proposals by foreign governments to mandate that Internet and telecommunications companies maintain, for between one and seven years, massive logs reflecting every innocent user's communications over their networks, or to mandate that companies install new surveillance technologies. The Council of Europe Cybercrime Convention that the U.S. Government helped to negotiate neither requires nor prevents such mandates.

The data retention mandates would require communications companies to retain enormous amounts of data that they do not retain in the ordinary course of business. Data would have to be retained about every user, without any showing that these users were suspected of engaging in illegal activity. The mandates would compromise user privacy, create costly barriers to entry for U.S. companies seeking to enter foreign markets, and threaten the security of user data by creating a ripe target for hackers. In some countries, such as Holland, service providers are subject to unique surveillance technology standards requirements, which create barriers to deploying international networks in those countries.

July 5, 2001

Honorable Lamar Smith
Chairman, Subcommittee on Crime
Committee on the Judiciary
House of Representatives
207 Cannon House Office Building
Washington, DC 20515
Attn: Veronica Eligan

Dear Congressman Smith,

Thank you for your recent letter with follow up questions to my June 14, 2001 testimony. I appreciate the opportunity to assist the committee further on this important issue, and have answered each question below. Please do not hesitate to contact me if I can be of assistance in the future.

1. *What are the types of cyber crime with which eBay is most concerned?*

Our concerns lay primarily in three areas. First, we are concerned with individuals who use the eBay site to steal money from others. In some cases, these individuals advertise goods and collect money from unsuspecting buyers with no intent of actually delivering merchandise. In other cases, individuals pay for merchandise with stolen credit cards or counterfeit cashier's checks, defrauding honest sellers. While such crime occurs in only a small percentage of our 6 million listings each week, they hurt not only our business but undermine public confidence in the internet as a safe place to do business.

Second, we are concerned with individuals who attempt to use eBay for unlawful purposes, such as selling counterfeit merchandise, prescription drugs, or items made from protected wildlife. We want our site to be a safe place for users around the world to conduct lawful business.

Third, we are concerned with individuals who interfere with our site operations, attacking our site with hacking or disruption programs or roboting stealing information from our site. Of particular concern are those individuals who use electronic robots to sweep our web site and steal email addresses from our users for the purpose of sending them unsolicited commercial emails.

2. *Is the Federal Government adequately working with you to deal with cyber*

crime?

Generally, we are quite pleased the outstanding efforts of federal law enforcement in this area. We have worked with virtually every federal law enforcement agency in the country, and found them to be highly professional and dedicated to fighting cyber crime. In some areas of the country, high prosecution minimums combined with inadequate punishment for some types of cyber crime and limited prosecution resources have caused law enforcement to decline prosecution of cases that should be prosecuted, and this is a problem that we believe needs to be addressed.

3. *Could you provide some examples of how you are working with law enforcement agencies in your efforts to reduce online auction fraud?*

eBay has a full time staff devoted solely to working with law enforcement in fighting crime on the Internet. This group sorts through reports of crime and proactively reaches out to law enforcement (using our own extensive database of knowledgable Internet law enforcement contacts around the world) to encourage prosecution of cases. They use tools developed inside eBay to quickly retrieve records (often within 24 hours) so that law enforcement gets what it needs fast, and they make certain information available to law enforcement without a subpoena, pursuant to our published privacy policies, speeding the investigation and greatly enhancing the chances that the perpetrator will be caught. One federal prosecutor in Illinois recently called our assistance program "phenomenal" and "surprising for a big company." Another federal prosecutor in Alabama noted that without our investigation support, the case in their district would never have been prosecuted.

eBay also promotes and subsidizes an online mediation program, which encourages users to resolve disputes themselves rather than involving law enforcement. When law enforcement involvement is needed, eBay works with both the FTC and the Internet Fraud Complaint Center to see that cases are promptly investigated.

We are also partnering with federal regulatory agencies to educate users about laws that might affect their ability to sell particular items. For example, eBay has given free web space on eBay to a number of federal agencies (including the Consumer Product Safety Commission, the FDA, the US Customs Service and others) so that the government can teach citizens about the law and prevent listings of improper items such as dangerous recalled products, viagra, freon, and other items.

4. *What recommendations do you have to improve investigations and prosecutions by federal law enforcement?*

Two things. One, give law enforcement the tools they need to do the job. This includes adequate funding for high tech crime task forces across the country with training and computer equipment, including prosecutors to do the work. Further, it including passing legislation that would increase the penalties for computer hacking cases and for fraud cases where large numbers of victims are involved. Such enhanced penalties encourage law enforcement to accept prosecution of such cases.

Second, law enforcement should take greater advantage of the regional high tech crime task force model, which brings state, local and federal law enforcement together with private industry to combat the problem.

5. *How does your Verified Rights Owners' Program protect intellectual property owners?*

eBay's Verified Rights Owner ("VeRO") Program helps Intellectual Property ("IP") and other rights owners protect their rights by enabling them to easily report potentially infringing listings to eBay. The VeRO Program counts among its members over 2300 companies and individuals representing every imaginable type of intellectual property - from major software companies to video game developers to the M.P.A.A. and R.I.A.A to the Salt Lake City Olympic Committee.

When an IP owner "joins" the VeRO program, eBay provides it with a form, called a Notice of Infringement ("NOI"). The NOI, tracks the notice requirements of the Digital Millennium Copyright Act ("DMCA"), and essentially requires the IP owner to identify itself and the item numbers of the potentially infringing listings. The IP owner can send eBay an NOI by fax, mail, or, after the first NOI, by email. Upon receiving an NOI from a rights owner, we expeditiously remove the offending listing (absent obvious error).

eBay's VeRO Program does not, however, rely solely on notices received from IP owners to identify infringing items being offered for sale through its site; eBay also searches its site daily for listings that appear on their face to be infringing. If a particular listing does not meet this "apparent infringement" standard, eBay tries to refer the listings to the rights owner for a determination.

To assist IP owners in searching for and identifying potentially infringing items, eBay offers IP owners an automated search tool called "Favorite Searches." With this tool, rights owners can have particular terms searched automatically on a daily basis. If the Favorite Searches tool finds any listings containing such terms, it will automatically email the search results to the IP owner.

Upon request, eBay also provides IP owners who are investigating IP infringements (or who wish to send demand letters to eBay users) with its Personal Information Agreement. After signing this agreement, eBay will provide the IP owner with personally identifying information concerning the user(s) at issue.

To further assist IP owners in protecting their rights, eBay suspends "repeat offenders" from the site, and endeavors to prevent such users from re-registering for the site. eBay's suspension policy tends to be a strict "two strikes and you're out" policy, but individual circumstances sometimes warrant suspension based upon only one offense. eBay employs a number of methods to keep suspended users from registering, including, among other things, credit card and other identification verification requirements, and various fraud profiling tools.

Finally, in order to actively deter the listing of potentially infringing items before a listing

is posted on the site, eBay has created special warning messages that appear every time a seller prepares to post any item in certain key categories. The warning message contains links to educational pages on our site that provide specific guidance relating to the offering of potentially infringing items. The warning messages also contain informational pages created solely by VeRO Program members. eBay also directs users to these pages in every email which eBay sends notifying a user that their listing has been ended early for infringement reasons.

6. *You described a program eBay created called the Fraud Assistance Team that works with law enforcement to assist in fraud cases. Does this include federal law enforcement and if so, what agencies?*

The Fraud Assistance team works with federal law enforcement agencies every day, most commonly with the Federal Bureau of Investigation, the US Postal Inspection Service, the US Customs Service, the US Fish and Wildlife Service and the US Secret Service. We have worked with virtually every federal agency that has criminal investigation responsibilities, including all branches of the military in the Department of Defense, the US Park Police, the US Marshals Service, the Food and Drug Administration, the Environmental Protection Agency, the Bureau of Indian Affairs, NASA, the Securities and Exchange Commission, the Internal Revenue Service and many others.

7. *Some prosecutors have expressed concern that the particular statutory approach for computing the minimum thresholds of damage in computer hacking cases, may in fact allow some significant criminals to go unpunished. Have you experienced problems where a minimum threshold of damage prevented the prosecution of fraud concuded on eBay? If so, how do you suggest we address this problem?*

Yes, eBay has experienced problems where computer intrusion cases against eBay were not prosecuted due to minimal penalties set out in Title 18, Section 1030 (a)(4) and (a)(5). Under the sentencing guidelines, an individual can severely disrupt Internet commerce, damaging not only the operators of commercial web sites but the businesses who rely on those sites for their livelihood, yet face little if any incarceration for their activities. In view of the importance of the Internet to the nation's economy, the penalties for individuals who intentionally disrupt Internet commerce should be increased, with penalties based on the length and economic severity of the disruption, taking into account the direct costs to the victim company and the indirect costs in lost business for the company and its customer.

Mr. Robert Chesnut
Vice President and Deputy Gneral Counsel
eBay, Incorporated

Business Software Alliance
www.bsa.org

July 16th, 2001

The Honorable Lamar Smith
Chairman
Subcommittee on Crime
Committee on the Judiciary
U.S. House of Representatives
Washington, DC 20515

Attn: Veronica Eligan, 207 Cannon

Dear Chairman Smith:

Thank you again for the opportunity to testify at the June 14th cybercrime hearing. I have previously transmitted my transcript edits and am enclosing my responses to the follow-up questions you submitted on June 28th.

Please let me know if I can be of any further assistance as you consider legislative changes to fight cybercrime.

Sincerely,

Bob Kruger
Vice President for Enforcement

Enclosure

1150 18th Street, N.W., Suite 700, Washington, D.C. 20036
TEL 202.872.5500 FAX 202.872.5501 EMAIL: software@bsa.org

Question 1
I understand BSA undertakes a significant amount of civil actions on its own.
a. Why are federal prosecutions under the "No Electronic Theft Act of 1998" and other copyright laws so important to stopping software piracy?
b. Could you comment on the federal prosecutions to date?
c. Apparently the number of prosecutions is very low, why is that the case and what can be done to raise the number?

Answer
Law enforcement actions are an integral part of the overall effort to combat software piracy for several reasons. First, criminal prosecutions powerfully communicate the importance that our society places on the creation of intellectual property. At a time when technology provides otherwise law-abiding individuals with means of inflicting great harm to the intellectual property rights of others and discussions rage over what is right or wrong in a digital age, prosecutions serve as a bright (red) light, demarcating the limits and helping to curb unlawful behavior. Second, criminal prosecutions are essential to deterring hardcore offenders who are not cowed by the prospect of a civil judgment or penalty. Third, law enforcement agents have investigative tools and capabilities that private parties lack.

Federal prosecutions are especially important to stopping software piracy because, unlike many other crimes, federal law enforcement agencies are the sole cop on the beat when it comes to prosecuting the NET Act and other forms of criminal copyright infringement. Due to federal pre-emption of copyright law, state and local law enforcement cannot prosecute copyright cases. Contrast theft of intellectual property to the car dealer who has cars stolen from his lot. The car dealer can call on all the resources of local, state, and federal law enforcement officials for assistance in tracking down and prosecuting the responsible party while he continues running his business.

BSA has been concerned for some time that the number of software piracy prosecutions, especially under the NET Act, have been too few and far between to inform public attitudes, let alone have a significant deterrent effect upon potential criminals. Most criminals know that stealing cars can and will bring jail time. Potential software thieves haven't gotten this message. We are encouraged by what appears to be an increase in recent months of the number of prosecutions announced at the Department of Justice web site during the first six months of the year and earnestly hope that this trend will continue.

We believe one reason for the paucity of prosecutions is the lack of clear direction to federal investigative agents and prosecutors in the field law from their supervisors and political leadership. I am not suggesting that NET Act cases or software copyright infringement should become a first or sole priority. But when only a handful of NET Act cases have been brought in the past three years, there is certainly room for improvement. In fact, investigating and prosecuting online piracy can often lead to the discovery of other criminal activity such as online fraud or child pornography and can help investigators develop online forensic skills useful in other areas.

Question 2
Please describe exactly how software piracy occurs.

Answer
Software piracy involves the unauthorized reproduction or distribution of copyrighted software programs. Piracy takes a number of forms ranging from end-user organizational piracy (where companies or organizations install more copies of software than they have licenses to support) to the sale of compilation CDs (on which dozens of programs can be compiled) to the production of sophisticated counterfeit packages designed to fool consumers into believing that the product is genuine. Of course, online piracy has the potential to make these "traditional" forms of piracy appear almost quaint by comparison. Pirated software made available for sale or downloading on the Internet can reach a global marketplace and is becoming increasing easy to find and obtain.

Question 3
You mention that BSA investigators do not have nor do they want surveillance capability. You state instead that intellectual property owners can and do use online tools, such as the Whois database that lists the registered owner of a website. You stated that sometimes this information is inaccurate or out of date and that the Committee might wish to look at this further. Please explain this recommendation in more detail.

Answer
Fighting online piracy is more difficult than in the offline world. Online pirates can run their operations from any location in the world and can use the anonymity afforded by the Internet to avoid detection. One important tool used by copyright owners to track down pirates is the Whois database -- which identifies the registered owner of a domain name. Sometimes a pirate web site uses its own domain name; other times pirates will use web-hosting services provided by larger ISPs.

In both cases, BSA investigators use Whois to contact those responsible for hosting pirated material on their computers. ICANN, the Internet's governing body, requires domain registrants to provide accurate Whois information when they register a domain. We have repeatedly come across Whois records that contain false or missing information. Examples include phone numbers listed as 911, non-existent towns in Alaska, and Whois records that include such street addresses as "007 Under Ground Lair." This Committee may wish to explore ways in which Whois records should be kept accurate. I would also point out that Whois records are not just used by intellectual property owners. They are used by local, state, and federal law enforcement in addition to consumer groups that use Whois to identify parties responsible for online fraud.

Question 4
In the past 12-18 months you stated you have seen a dramatic increase in the amount of high quality counterfeit software imported into the U.S. from overseas, especially Asia. What is the percentage increase?

Answer
Although an exact percentage increase is difficult to quantify, it is worth noting two relevant facts. First, BSA members have seen an increase in the total number of counterfeit product seizures by US Customs as counterfeiters break up their shipments into smaller lots to avoid detection by law enforcement. Second, a result of this increased effort to avoid detection is that more counterfeit product is slipping past undetected since only a small percentage of import shipments undergo can be inspected. In the past three years, worldwide counterfeit software seizures have totaled in excess of $500 million in value compared to slightly more than $125 million in the United and Canada.

Question 5
What does piracy cost the software industry, in terms of dollars, on an annual basis?

Answer
Every year, the Business Software Alliance hires an outside firm, International Planning and Research to conduct a worldwide survey of software piracy. This survey has been conducted since 1994. A full copy of the IPR study can be found at the BSA website at www.bsa.org and a copy of it is attached. In short, piracy in the US costs the software industry $2.6 billion last year. Worldwide, the cost is much greater, $11.75 billion. Although piracy rates have fallen over the years in most countries, the cost of software piracy has remained somewhat constant as the size of the market has grown.

Question 6
Do you work with federal, local and state law enforcement in your efforts against piracy?
a. Would you describe your work with them as helpful?
b. Do you have any suggestions on better cooperation and coordination?

Answer
BSA works extensively with law enforcement agencies at all levels although, as noted above, state and local copyright prosecutions are preempted by federal law. BSA participates in training programs for agents and prosecutors, develops and refers cases and provides support for ongoing investigations. For example, this May, BSA's Manager of Investigations testified in the first jury trial under the NET Act. The defendant, a member of the Pirates With Attitude software ring, was found guilty.

Since the number of prosecutions has been so low, BSA's main focus has been increasing the number of cases brought. We have worked with the various coordinating units and bodies, such as DOJ's Computer Crimes and Intellectual Property Section, the National Intellectual Property Law Enforcement Coordinating Council and the Joint FBI-Customs IPR Center to bring this about. In addition to the need for a strong direction from above, it is of course necessary to ensure adequate funding to support these prosecutions. We are pleased to see that the House of Representatives has specifically mentioned the need for greater intellectual property prosecutions in the FY02 budget.

Question 7
Mr. Miller, President of the Information Technology Association of America, testified that cyber crime is a threat to the digital economy. How serious of a threat do you believe there is with regard to software companies?

Answer
BSA has long faced the issue of piracy of digital goods since software has always and only been available in digital form. The threat is growing as more of the world's Internet users employ high-speed access to the Internet to exchange infringing content. If publishers cannot obtain a return on the very substantial investment of money, time, and creativity they make in the development of software programs, they will have no ability or incentive to create new products.

American's software companies are second to none in the world and their exports contribute to a substantial positive trade flow. Cybercrime threatens not only our companies' bottom lines, but also an important part of our nation's domestic and trading economy.

Sixth Annual BSA Global Software

Piracy Study

May 2001

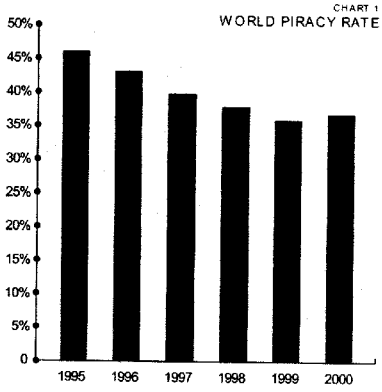
Sixth Annual BSA Global Software

Piracy Study

In early 2001, International Planning and Research Corporation (IPR) completed another year of analysis in an ongoing study for the Business Software Alliance (BSA) and its member companies. The purpose of the study is to review the available data and utilize a systematic methodology to determine the worldwide business software piracy rates and the associated dollar losses.

A. OVERVIEW

CHART 1
WORLD PIRACY RATE



The results from the annual BSA Global Piracy Study for 2000 indicate that software piracy continued to pose challenges for the industry and the global economy. For the first time in the study's history, the world piracy rate in 2000 did not decline, but instead showed a slight increase to 37%. The dollar losses due to piracy declined 3.5% from 1999 to $11.75 billion. This decline in dollar terms is not an indication of a decrease in piracy. It is, in fact, the result of several other factors. The U.S. dollar was strong in 2000. Software prices continued to fall, advancing a trend of declining prices that has evolved over the last decade. In addition, the overall market for software grew at the slowest rate since the study started in 1994. The combination of slow growth and somewhat lower prices resulted in a slight reduction in the dollar losses due to piracy. But at $11.75 billion, it is no small problem.

In past studies, IPR has cited several reasons for the decline in software piracy. These include:

1. As PC technology and the demand for software spread from the U.S. to other countries during the 1990's, there was at times a lag between the demand for software and the effective distribution of legal software. This led to cases of piracy as an expedient way to use PCs. The software industry has worked hard to have a legitimate sales presence in every country, making legal software sales and support easier to obtain.
2. Software companies have increased the availability of user support for their products outside of the U.S. This increased user support has promoted the purchase of legal software.
3. Prices for original software have declined over the past decade, making the benefits of original software more compelling against the risks of software piracy.
4. The BSA and other organizations have promoted the need to purchase legal versions of software and the importance of intellectual property rights. This has included high-profile legal actions against companies using illegal software.
5. In an increasingly global marketplace, a company's risk of being caught using illegal software extends beyond the legal implications and includes their business practices and credibility.
6. Efforts to increase government cooperation to provide legal protection for intellectual property and to criminalize software piracy have also assisted in stemming the growth of piracy.

Unfortunately, this downward trend in piracy rates may be ending. 2000 was a year of relatively slow growth and also a year of steady piracy overall. It appears that there is more change in the attitudes toward piracy in periods of economic growth, when businesses are adapting new technology to keep up with demand and competitive pressures, than in times of slower growth.
It also points to a fundamental piracy problem in the more technologically advanced regions, specifically North America and Western Europe. Countries in these regions have either showed small declines in their piracy rates or constant or increasing piracy

rates. Although these regions have the lowest piracy rates in the world, they are showing the least progress in reducing piracy. This suggests a core piracy problem that is more entrenched and, therefore, more difficult to overcome.

Another factor that kept the piracy rates from falling in 2000 is that the fastest growing regions were the ones with the highest piracy rates. The world piracy rate did not decline in 2000. Growth in the Asia-Pacific region, with its higher piracy rate, offset declines elsewhere. In the future, IPR expects growth in the more rapidly developing regions to continue. Consequently, relatively higher piracy rates will become a larger problem.

Many regions experienced smaller dollar losses in 2000 compared to 1999. A combination of slow growth and somewhat lower prices for software slightly reduced the dollar losses due to piracy. Dollar losses rose in the Asia/Pacific region, growing to over $4 billion for the first time. In fact, it was the region with the highest dollar losses in 2000. Western Europe was second with slightly more than $3 billion in losses. North America was third with just under $3 billion in losses, its lowest ranking since 1995, when it also ranked third in dollar losses.

There were no significant shifts in piracy in 2000. Eastern Europe, at 63%, was the region with the highest piracy rate. Eastern Europe has been the region with the highest piracy rate in every study since 1994. Latin America became the region with the second highest piracy rate in 2000 at 58%, ahead of the Middle East at 57%. In past years, the piracy rate in the Middle East had exceeded the rate in Latin America.

The North American region continued to be the area with the lowest piracy rate at 25%, a slight decline over 1999. Western Europe continued as the region with the second lowest piracy rate at 34%, and showed the smallest year-over-year change in piracy of any region. Both North America and Western Europe are not experiencing significant decreases in their piracy rates from year to year and appear to be establishing a more consistent level of piracy. While other successes have been recognized, this unfortunate trend indicates that there is a core piracy problem that is harder to solve.

The Asia/Pacific region was the only region that increased its rate of piracy in 2000, rising to 51%. This is also an unfortunate trend and contrary to the general improvement in the piracy rates documented in this study since 1994.

Africa had a four percentage point drop in the piracy rate. In 2000, it was 52%, down from 56% in 1999. While encouraging, it is uncertain that improvements in the piracy rate will continue in the future, as the change may be the result of temporary conditions. Sustained declines in piracy would provide evidence of a more substantial change in software practices.

CHART 2

DOLLAR LOSSES BY REGION (BILLIONS)

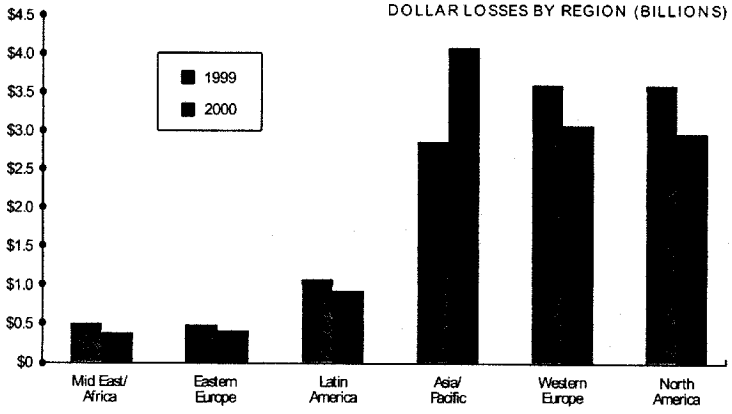
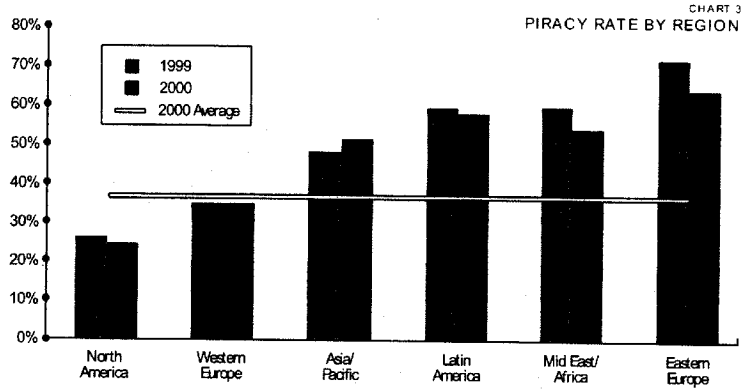


CHART 3
PIRACY RATE BY REGION



B. THE TOP OFFENDERS

Table 1
Top 25 Countries by Piracy Rate

	1999	2000
Vietnam	98%	97%
China	91%	94%
Indonesia	85%	89%
Ukraine/Other CIS	90%	89%
Russia	89%	88%
Lebanon	88%	83%
Pakistan	83%	83%
Bolivia	85%	81%
Qatar	80%	81%
Bahrain	82%	80%
Kuwait	81%	80%
Thailand	81%	79%
El Salvador	83%	79%
Nicaragua	80%	78%
Oman	88%	78%
Bulgaria	80%	78%
Romania	81%	77%
Guatemala	80%	77%
Paraguay	83%	76%
Jordan	75%	71%
Honduras	75%	68%
Costa Rica	71%	68%
Dominican Republic	72%	68%
Kenya	67%	67%
Nigeria	68%	67%

WESTERN EUROPE

Greece remained the country in Western Europe with the highest piracy rate at 66%. Denmark and the United Kingdom were the two countries with the lowest piracy rates, at 26%.

Several countries in Western Europe did not experience lower piracy rates in 2000, including some of the largest markets, such as France, Germany, the U.K., Austria, Italy, Sweden, and Switzerland. This is a departure from the general trend of lower piracy rates that have been observed since 1994, and could represent a disturbing trend for the future.

EASTERN EUROPE

Russia and the Ukraine/Other CIS countries continued to have the highest piracy rates in Eastern Europe in 2000 with 88% and 89%, respectively.

Poland, the third largest country in the region, had the largest reduction in the piracy rate, down six percentage points to 54%. The Czech Republic continued to have the lowest piracy rate at 43%.

NORTH AMERICA

Both the United States and Canada experienced declines in the piracy rate in 2000, with the U.S. at 24%, the lowest in the world, and Canada at 38%.

LATIN AMERICA

Latin America experienced a small decline in the average piracy rate in 2000. The piracy rates in Brazil and Mexico, the two largest economies in the region, remained unchanged, at 58% and 56%, respectively. The piracy rate in Argentina, the third largest economy in the region, was also at 58% in 2000.

Chile was again the country with the lowest piracy rate in Latin America, at 49%. Bolivia was again the country with the highest piracy rate, at 81%.

ASIA/PACIFIC

Several large countries in Asia experienced increases in their piracy rates in 2000. For example, Japan's rate increased to 37%, China's rate increased to 94%, and Korea's rate increased to 56%.

Several other countries showed very little changes in their piracy rates in 2000. India had a 63% piracy rate, up from 61% in 1999. Hong Kong had a 57% piracy rate, up from 56% in 1999. Australia had a 33% piracy rate, up from 32% in 1999.

New Zealand, with a 28% piracy rate in 2000, continued as the country with the lowest piracy rate in the Asia/Pacific region. Vietnam, with a piracy rate at 97%, continued as the country with the highest piracy rate in the region. China, with 94%, followed as the country with the second highest piracy rate.

MIDDLE EAST

The three largest economies in the Middle East, Turkey, Israel, and Saudi Arabia, each saw a decrease in the piracy rate in 2000, with Turkey dropping the most, from 74% in 1999 to 63% in 2000. Israel, with a 41% piracy rate, was the country with the lowest piracy rate in the region. Bahrain, Kuwait, and Qatar each had more than an 80% piracy rate in 2000.

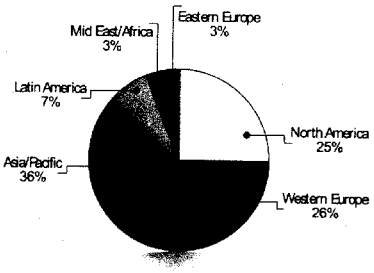
AFRICA

Africa saw a decline in the piracy rate, from 56% in 1999 to 52% in 2000. South Africa, the largest economy in the region, had the lowest piracy rate, at 45%. Kenya and Nigeria were the two countries with the highest piracy rate, both at 67% in 2000.

C. ALLOCATION OF LOSSES

CHART 4

DOLLAR LOSSES BY REGION, 2000



As Chart 4 shows, the regions with the highest dollar losses in 2000 were Asia/Pacific, Western Europe, and North America. These regions have the largest economies and correspondingly, the largest PC and software markets. Their relatively low piracy rates still translate into large dollar losses, although the Asia/Pacific region, with a substantially higher piracy rate than North America or Western Europe, made up 36% of the world losses due to piracy.

The dollar losses declined in North America from 1994 to 2000 by nearly $1 billion, but they increased in Asia/Pacific by $900 million, and in Western Europe by $300 million. Dollar losses fell in the slow growth environments of Latin America, Eastern Europe, the Middle East and Africa. The declines in these areas were largely due to the economic slowdowns of these regions, and are not expected to continue as they recover.

In the U.S., the piracy rate declined to 24% in 2000, from 31% in 1994. This is the lowest rate of any country, but still represents a dollar loss of $2.6 billion. In Western Europe, Germany and the United Kingdom had the highest dollar losses with $635 million and $531 million, respectively, even though their piracy rates were measured at 28% for Germany and 26% for the UK. France was third with $481 million in dollar losses, driven in part by France's substantially higher piracy rate of 40%.

D. 2000 BSA PIRACY STUDY RESULTS

	Piracy Rates						Retail Software Revenue Lost to Piracy (1000)					
	1995	1996	1997	1998	1999	2000	1995	1996	1997	1998	1999	2000
WESTERN EUROPE												
Austria	47%	43%	40%	38%	36%	37%	$66,994	$50,267	$41,620	$51,164	$66,929	$70,748
Belgium/Luxembourg	48%	38%	36%	35%	36%	33%	$78,210	$49,197	$51,485	$53,401	$77,372	$53,767
Denmark	47%	35%	32%	31%	29%	26%	$82,670	$37,531	$45,787	$42,069	$59,184	$40,076
Finland	50%	41%	38%	32%	30%	29%	$80,604	$36,335	$37,754	$36,126	$50,594	$39,135
France	51%	45%	44%	43%	39%	40%	$537,567	$411,966	$407,900	$425,205	$548,408	$480,604
Germany	42%	36%	33%	28%	27%	28%	$775,898	$497,950	$508,884	$479,367	$652,379	$635,264
Greece	86%	78%	73%	74%	71%	66%	$40,573	$45,802	$44,546	$55,385	$67,708	$61,542
Ireland	71%	70%	65%	56%	51%	41%	$40,640	$45,650	$46,847	$60,986	$117,892	$77,399
Italy	61%	55%	43%	45%	44%	46%	$503,648	$340,784	$271,714	$356,879	$421,434	$421,942
Netherlands	63%	53%	48%	45%	44%	40%	$275,320	$221,144	$195,098	$195,778	$264,400	$227,595
Norway	54%	54%	46%	40%	37%	35%	$96,981	$103,852	$104,337	$72,452	$87,568	$64,292
Portugal	61%	53%	51%	43%	47%	42%	$50,230	$36,183	$40,991	$36,109	$49,920	$23,609
Spain	74%	65%	59%	57%	53%	51%	$229,933	$148,823	$167,288	$235,100	$247,650	$168,514
Sweden	54%	47%	43%	38%	35%	35%	$206,332	$112,498	$127,051	$119,073	$131,358	$92,889
Switzerland	47%	43%	39%	33%	33%	34%	$132,779	$99,545	$92,898	$76,471	$107,068	$91,093
UK	38%	34%	31%	29%	26%	26%	$444,561	$337,344	$334,527	$464,771	$679,506	$530,787
TOTAL W. EUROPE	**49%**	**43%**	**39%**	**36%**	**34%**	**34%**	**$3,642,939**	**$2,574,871**	**$2,518,726**	**$2,760,337**	**$3,629,371**	**$3,079,256**
EASTERN EUROPE												
Bulgaria	94%	98%	93%	90%	80%	78%	$20,394	$9,594	$13,171	$17,746	$11,245	$10,019
Croatia	91%	79%	69%	64%	60%	63%	$18,072	$7,715	$7,569	$10,373	$4,061	$8,384
Czech Rep.	62%	53%	52%	45%	42%	43%	$56,108	$69,212	$51,972	$43,261	$36,897	$44,674
Hungary	73%	69%	58%	57%	52%	51%	$55,086	$42,987	$25,488	$38,465	$37,262	$41,252
Poland	75%	71%	61%	61%	60%	54%	$150,287	$169,202	$107,625	$142,484	$164,914	$103,531
Romania	93%	86%	84%	86%	81%	77%	$20,163	$8,380	$15,297	$21,530	$12,132	$20,918
Russia	94%	91%	89%	92%	89%	88%	$301,076	$383,304	$251,837	$273,055	$165,515	$108,983
Slovakia	62%	56%	58%	50%	46%	45%	$13,678	$14,055	$17,018	$11,241	$9,653	$6,866
Slovenia	96%	91%	76%	73%	70%	61%	$20,174	$8,666	$9,198	$12,223	$10,366	$11,743
Ukraine/Other CIS	94%	95%	92%	93%	90%	89%	$37,033	$49,469	$44,276	$47,477	$43,520	$29,700
Other Eastern Europe	83%	72%	61%	56%	52%	52%	$56,006	$19,924	$17,905	$22,160	$9,647	$18,423
TOTAL E. EUROPE	**83%**	**80%**	**77%**	**76%**	**70%**	**63%**	**$748,077**	**$782,508**	**$561,356**	**$640,015**	**$505,213**	**$404,491**
NORTH AMERICA												
US	26%	27%	27%	25%	25%	24%	$2,940,294	$2,360,934	$2,779,673	$2,875,185	$3,191,111	$2,632,438
Canada	44%	42%	39%	40%	41%	38%	$347,085	$357,316	$294,593	$320,636	$440,101	$304,999
TOTAL US/CANADA	**27%**	**28%**	**28%**	**26%**	**26%**	**25%**	**$3,287,379**	**$2,718,251**	**$3,074,266**	**$3,195,821**	**$3,631,212**	**$2,937,437**
LATIN AMERICA												
Argentina	80%	71%	65%	62%	62%	58%	$151,814	$122,389	$105,194	$123,786	$192,001	$114,403
Bolivia	92%	89%	88%	87%	85%	81%	$4,017	$3,527	$3,853	$4,898	$5,059	$3,470
Brazil	74%	68%	62%	61%	58%	58%	$441,592	$356,370	$394,994	$366,688	$392,031	$325,617
Chile	68%	62%	56%	53%	51%	49%	$47,920	$39,960	$33,147	$39,451	$58,479	$40,726
Columbia	72%	66%	62%	60%	58%	53%	$103,288	$85,920	$65,085	$83,615	$61,843	$40,924
Costa Rica	89%	82%	74%	72%	71%	68%	$7,303	$6,735	$7,064	$8,392	$11,545	$18,344
Dominican Republic	89%	80%	76%	73%	72%	68%	$7,172	$5,473	$7,647	$9,019	$15,267	$8,206
Ecuador	88%	80%	75%	73%	71%	65%	$15,460	$12,852	$13,236	$15,619	$25,142	$10,125
El Salvador	97%	92%	89%	87%	83%	79%	$13,207	$11,489	$10,419	$12,949	$16,697	$11,944
Guatemala	94%	89%	86%	85%	80%	77%	$10,095	$8,675	$7,867	$9,357	$15,580	$15,115
Honduras	88%	83%	78%	77%	75%	68%	$4,592	$3,918	$3,468	$4,254	$6,280	$2,431
Mexico	74%	67%	62%	59%	56%	56%	$135,905	$105,909	$133,102	$147,138	$133,964	$180,164
Nicaragua	92%	89%	83%	81%	80%	78%	$6,529	$5,763	$5,010	$6,144	$6,773	$2,579
Panama	77%	74%	72%	70%	66%	64%	$7,330	$6,434	$5,859	$7,004	$12,832	$10,087
Paraguay	95%	89%	87%	85%	83%	76%	$6,327	$5,408	$5,029	$6,371	$8,198	$10,433
Peru	84%	74%	66%	64%	63%	61%	$40,522	$32,437	$31,017	$37,462	$27,210	$15,573
Puerto Rico	71%	50%	49%	49%	48%	46%	$24,282	$17,402	$18,826	$22,874	$24,956	$13,766
Uruguay	84%	79%	74%	72%	70%	66%	$18,876	$16,116	$13,613	$16,109	$19,608	$9,688
Venezuela	72%	70%	64%	62%	60%	58%	$57,968	$51,272	$54,905	$68,298	$56,823	$20,792
Other Latin America	78%	75%	75%	72%	72%	67%	$37,317	$82,518	$58,658	$56,081	$37,351	$15,390
TOTAL LATIN AMERICA	**76%**	**69%**	**64%**	**62%**	**59%**	**58%**	**$1,141,516**	**$980,568**	**$977,994**	**$1,045,506**	**$1,127,639**	**$869,777**

	Piracy Rates						Retail Software Revenue Lost to Piracy (1000)					
	1995	1996	1997	1998	1999	2000	1995	1996	1997	1998	1999	2000
ASIA/PACIFIC												
Australia	35%	32%	32%	33%	32%	33%	$198,146	$128,267	$129,414	$192,237	$150,390	$132,533
China	96%	96%	96%	95%	91%	94%	$443,933	$703,839	$1,449,454	$1,193,386	$645,480	$1,124,395
Hong Kong	62%	64%	67%	59%	56%	57%	$122,938	$129,109	$122,169	$88,627	$110,190	$86,195
India	78%	79%	69%	65%	61%	63%	$155,645	$255,344	$184,664	$197,333	$214,557	$239,629
Indonesia	98%	97%	93%	92%	85%	89%	$150,921	$197,313	$193,275	$58,756	$42,106	$69,991
Japan	55%	41%	32%	31%	31%	37%	$1,648,493	$1,190,323	$752,598	$596,910	$975,396	$1,666,331
Korea	76%	70%	67%	64%	50%	56%	$675,281	$515,547	$582,320	$197,516	$197,269	$302,938
Malaysia	77%	80%	70%	73%	71%	66%	$80,596	$121,488	$82,552	$79,268	$84,154	$95,567
New Zealand	40%	35%	34%	32%	31%	28%	$26,083	$29,271	$20,284	$21,758	$19,656	$12,373
Pakistan	92%	92%	88%	86%	83%	83%	$14,233	$23,144	$20,395	$22,667	$18,913	$31,379
Philippines	91%	92%	83%	77%	70%	61%	$45,022	$70,735	$49,151	$31,138	$33,163	$27,091
Singapore	53%	59%	56%	52%	51%	50%	$40,374	$56,553	$56,599	$58,262	$61,758	$44,299
Taiwan	70%	66%	63%	59%	54%	53%	$165,462	$116,980	$136,850	$141,274	$122,946	$154,754
Thailand	82%	80%	84%	82%	81%	79%	$99,146	$137,063	$94,404	$48,613	$82,183	$53,082
Vietnam	99%	99%	98%	97%	98%	97%	$35,076	$15,216	$10,132	$10,328	$13,106	$34,938
Other Asia/Pacific	95%	86%	83%	74%	71%	75%	$90,053	$49,113	$31,974	$16,739	$20,262	$7,566
TOTAL ASIA/PACIFIC	**64%**	**55%**	**52%**	**49%**	**47%**	**51%**	**$3,991,399**	**$3,739,304**	**$3,916,236**	**$2,954,812**	**$2,791,531**	**$4,083,061**
MIDDLE EAST/AFRICA												
Bahrain	92%	90%	89%	89%	82%	80%	$4,243	$4,495	$3,576	$3,012	$6,021	$4,745
Cyprus	77%	70%	68%	68%	67%	63%	$2,566	$2,540	$1,809	$1,518	$3,345	$2,382
Israel	75%	69%	54%	48%	44%	41%	$55,639	$77,261	$57,060	$63,239	$72,487	$66,256
Jordan	87%	83%	80%	80%	75%	71%	$2,567	$2,659	$1,883	$1,584	$3,276	$2,116
Kuwait	91%	89%	88%	88%	81%	80%	$10,300	$10,817	$7,889	$6,644	$13,200	$8,143
Lebanon	91%	88%	93%	93%	88%	83%	$1,643	$1,708	$1,322	$1,119	$2,059	$1,600
Malta	77%	70%	64%	63%	58%	56%	$1,975	$1,956	$1,299	$1,090	$2,220	$1,667
Mauritius	90%	88%	77%	78%	70%	66%	$1,562	$1,646	$1,070	$902	$1,263	$1,482
Oman	96%	95%	93%	93%	88%	78%	$7,397	$7,905	$5,682	$4,784	$9,780	$6,535
Qatar	91%	89%	87%	87%	80%	81%	$3,033	$3,206	$2,760	$2,325	$4,451	$3,736
Reunion	72%	66%	59%	59%	54%	49%	$1,894	$1,860	$1,232	$1,036	$1,458	$1,881
Saudi Arabia	77%	79%	74%	73%	64%	59%	$59,724	$65,192	$46,156	$38,768	$39,900	$21,671
Turkey	90%	85%	84%	87%	74%	63%	$95,249	$90,717	$64,306	$55,823	$98,257	$96,472
UAE	86%	50%	50%	49%	47%	44%	$9,558	$6,026	$4,420	$3,637	$7,624	$5,393
Other Middle East	78%	73%	73%	73%	69%	63%	$7,470	$7,534	$5,538	$4,661	$19,103	$16,372
TOTAL MIDDLE EAST	**83%**	**79%**	**72%**	**69%**	**63%**	**57%**	**$264,820**	**$285,522**	**$206,003**	**$190,139**	**$284,445**	**$240,451**
Egypt	84%	88%	85%	85%	75%	56%	$10,674	$18,128	$12,890	$10,858	$33,197	$12,232
Kenya	82%	77%	72%	72%	67%	67%	$437	$443	$302	$254	$372	$2,805
Morocco	82%	77%	72%	72%	64%	60%	$6,579	$6,675	$4,559	$3,829	$5,267	$6,045
Nigeria	82%	77%	72%	72%	67%	67%	$3,620	$3,673	$2,509	$2,107	$2,951	$3,247
South Africa	58%	49%	48%	49%	47%	45%	$88,323	$43,783	$69,833	$94,241	$84,149	$54,447
Zimbabwe	59%	70%	66%	67%	63%	59%	$576	$717	$699	$810	$845	$508
Other Africa	86%	83%	71%	69%	66%	62%	$146,302	$151,814	$94,715	$77,781	$66,966	$56,607
TOTAL AFRICA	**74%**	**70%**	**60%**	**58%**	**56%**	**52%**	**$256,512**	**$225,234**	**$185,507**	**$189,881**	**$193,747**	**$135,892**
TOTAL MID EAST/ AFRICA	**78%**	**74%**	**65%**	**63%**	**60%**	**55%**	**$521,332**	**$510,756**	**$391,510**	**$380,020**	**$478,192**	**$376,344**
TOTAL WORLD	46%	43%	40%	38%	36%	37%	$13,332,642	$11,306,258	$11,440,088	$10,976,511	$12,163,158	$11,750,365

E. BSA GLOBAL PIRACY STUDY METHODOLOGY

Developed by International Planning and Research (IPR)

The BSA Global Piracy Study involves the reconciliation of two sets of data, the demand for new software applications and the legal supply of new software applications. IPR developed the following method to estimate software piracy by country. This study is for the calendar year 2000.

DEMAND

PC shipments for the major countries were estimated from proprietary and confidential data supplied by BSA member companies. The data was compared and combined to form a consensus estimate, which benefited from the detailed market research available to these member companies.

To analyze demand, PC shipments were studied in two dimensions: (1) home vs. non-home segments, and (2) replacement PCs vs. new units. Splitting the PC shipments between home and non-home purchasers represented the market segments of each country. The PC shipments were also compared to the change in the installed base of existing PCs. The part of PC shipments, which represents growth of the installed base, is called "new shipments" and is separated from the "replacement shipments." Replacement shipments represent new PCs that are replacing older PCs.

IPR also developed a measure of the installed base of PCs by country compared to the number of white-collar workers. PC penetration statistics are a general measure of the level of technological acceptance within a country. The level of penetration, for a variety of reasons, varies widely from country to country. This level was then ranked and each country was assigned to one of five maturity classes.

From market research provided by member companies, IPR determined the number of software applications installed per PC shipment and developed these ratios for the four shipment groups:

1. Home - New Shipments
2. Non-Home - New Shipments
3. Home - Replacement Shipments
4. Non-Home - Replacement Shipments

For each shipment group, ratios were developed for each of five maturity classes. U.S. historical trends were used to estimate the effects of slowed technological development by maturity class.

Piracy rates can vary among applications. Grouping the software applications into three tiers and using specific ratios for each tier further refined the ratios. The tiers used were General Productivity Applications, Professional Applications, and Utilities. These were chosen because they represent different target markets, different price levels, and it is believed, different piracy rates.

As part of this study, software applications installed per PC shipped have been researched and estimated using these dimensions:

1. Home vs. Non-Home
2. New PCs vs. Replacement PCs
3. Level of Technological Development
4. Software Application Tier

From this work, an estimate of total installed software applications was calculated by country for each software tier. This produced a figure for total worldwide software installed in 2000, both legal and illegal.

SUPPLY

For the 1995 and 1996 piracy studies, the primary source of data for software shipments was the Software and Information Industry Association (SIIA) Data Program. However, the SIIA Data Program ceased operation in 1997. The challenge for the subsequent studies has been to replace that data source.

IPR's approach was to utilize the member companies of BSA to develop piracy study sponsors who would volunteer their proprietary shipment data to the study under non-disclosure agreements for the purpose of constructing an accurate estimate of the software industry's 2000 shipments. This became the primary source of software shipment data.

Because the SIIA Data Program was active until early 1997, IPR is able to continue using it to provide historical estimates of the software industry and can calibrate the results of the data collection from our sponsors in determining software shipments for the total industry. This has been IPR's crosscheck and leads us to believe that our data collection provided reliable and consistent estimates.

The data was collected by country and by software application. For this study, only business software applications were used, hence, seven consumer software applications were excluded:

1. Recreation
2. Home Creativity
3. Home Education
4. Integrated
5. Personal Finance
6. Reference Software
7. Tax Programs

The 26 business software applications are:

TIER 1—General Productivity Applications

1. Databases
2. Presentations Graphics
3. Project Management
4. Spreadsheets
5. Word Processors

TIER 2—Professional Applications

6. Accounting
7. C Languages
8. Curricular
9. Desktop Publishing
10. Other Languages
11. Professional Drawing and Painting
12. Programming Tools

TIER 3—Utilities

13. Application Utilities
14. Calendars & Scheduling
15. Clips
16. Communications
17. Education Administration & Productivity
18. Electronic Mail
19. Fonts
20. Forms
21. General Business
22. Internet Access and Tools
23. Personal and Business Productivity
24. PIM's
25. System Utilities
26. Training

The collected software shipment data represent the software shipments of most U.S. companies. To estimate the entire U.S. software shipments, IPR used an uplift factor reflecting an estimate of shipments by companies participating in the study as a percent of software shipped by all U.S. software publishers.

To estimate the entire worldwide software shipments, IPR applied a second uplift factor, based on an estimate of software shipped by U.S. companies as a percent of software shipped by all software publishers.

FACTOR 1:

Software shipped by the piracy study participating companies as a percent of software shipped by all U.S. software publishers.

FACTOR 2:

Software shipped by U.S. software publishers as a percent of software shipped by all software publishers.

By applying these two factors, we are able to estimate the total legal market of software shipments for all companies.

IPR believes that certain software shipments in the data collected from participating companies are reported for one country, but the software is exported and used in another country. In order to account for this and to eliminate this effect from the piracy study as much as possible, net import estimates were developed on a country-by-country basis.

PIRACY ESTIMATES

The difference between software applications installed (demand) and software applications legally shipped (supply) equals the estimate of software applications pirated. These were calculated by country for 2000. The piracy rate was defined as the volume of software pirated as a percent of total software installed in each country.

By using the average price information from the collected data, the legal and pirated software revenue was calculated. This is a wholesale price estimate weighted by the amount of shipments within each software application category.

REST OF REGION COUNTRIES

The "rest of region" data was used to develop piracy estimates outside of the major markets. The methodology for the piracy study provides total world shipments with country information for the major countries and aggregated information for smaller countries. For these additional countries, a PC shipment estimate was acquired, either through a consensus of member company internal data or from published sources. This data was used to split apart the "rest of region" total for the countries within each region.

Wherever possible, separate software shipment data was used to split the software shipments within the "rest of region" countries. This resulted in piracy estimates that varied by country within the region. Where this data was unavailable, the additional countries have the same piracy rate as the region.

REVIEW PROCESS

To ensure a high level of confidence, member companies of BSA reviewed the results of the study and their input was used to validate and refine the study assumptions.