Remarks of Deputy Attorney General Eric H. Holder, Jr.

High-Tech Crime Summit

January 12, 2000

Hyatt Regency Capitol Hill
400 New Jersey Avenue, NW
Washington, DC

I would like to thank you for inviting me to address this high-tech crime summit. The issue of high-tech crime -- and the challenges it poses to law enforcement -- are among the highest priorities for the Department of Justice and for me personally.

I also want to commend you for bringing together such an important -- and potentially influential -- group of industry and high-tech crime-fighting experts. Perhaps more than in any other area of crime, our success in preventing and prosecuting high-tech crime turns, in large part, on the effectiveness of the relationships and partnerships we form between law enforcement and industry. Today, I encourage you to move beyond the discussion of "why" high-tech crime should be at the top of the government and industry's agenda and to focus on "how" we can develop a more effective response.

Overview of Remarks

Today, I would like to touch upon some of the challenges that we -- that is, the law enforcement community -- are facing in the Information Age. Next, I will outline some of the specific steps that we are taking to combat high-tech crime, particularly crime involving the theft of intellectual property -- which is of particular concern to this nation's high-tech economy. Finally, I will conclude with some concrete suggestions on how industry can assist us in this effort and I will invite you to identify how the Department of Justice can assist you in protecting our high-tech companies against crime.

The Nature and Extent of High-Tech Crime?

How big is the computer and high-tech crime problem? We simply don't know. We do know that computer crime costs industry and society billions of dollars every year. There is substantial evidence computer crime is increasing in scope and in complexity. And we know that, left unchallenged, computer crime will stifle the expansion of electronic commerce and, potentially, pose a serious threat to public health and safety, particularly when we look at the vulnerability of critical infrastructures, such as the air traffic control system, the power grid, and national defense systems -- all of which are totally dependent on computer networks.

Law Enforcement Challenges in the Information Age

The Information Age -- that is the integration of information technologies into virtually every aspect of business and society -- is posing new challenges for law enforcement, both domestically and around the globe. While the Internet and other information technologies provide enormous benefits to society in the areas of commerce, health care, education, and the like, they also provide new opportunities for criminal behavior. Generally, these crimes fall into three areas:

First, there are crimes where the computer is the target -- so-called hacking or intrusion crimes.

Second, there are crimes where computers are the medium by which the criminal conduct is committed. This would include software piracy, Internet fraud, and telephone toll fraud.

Third, we see many crimes where computers are used incidentally to the criminal offense, such as when drug traffickers store information on computers or where the evidence of health care fraud or other white collar crimes are stored on computer networks.

While these three categories cover most forms of computer crime, and include many crimes such as software piracy and intrusion cases that are of concern to the high-tech industry, we also realize that some traditional forms of criminal activity -- such as cargo theft -- are a major problem for industry.

What Are the Challenges?

Crimes involving information technologies pose new challenges for law enforcement. First, the Internet and other computer systems do not recognize state or international boundaries. An individual who is "armed" with nothing more than a computer and modem can victimize individuals and businesses anywhere in the world without ever stepping foot outside his or her home. While the Internet may be borderless, law enforcement agencies must respect the sovereignty of other nations. As a result, we increasingly are dedendent on cooperation with foreign law enforcement agencies in fighting computer crime. Unfortunately, differing legal systems and a significant disparity in technical expertise among foreign law enforcement agencies are major obstacles in our efforts.

Second, anonymity increasingly is possible on the Internet. While less sophisticated cybercriminals may leave electronic "footprints," more experienced criminals know how to conceal their tracks in cyberspace. With the widespread deployment of anonymous software, it will be difficult or impossible to trace cybercriminals. Anonymity poses challenges in a number of areas, particularly in the area of software piracy.

Third, the identification and location of computer criminals can be extremely difficult. Today, a single communication may be routed through a U.S. cable company or ISP, across the Atlantic via satellite, and across Europe via a wireless phone network. A trace of such a communication will require the cooperation of numerous U.S. and foreign telecommunication companies and law enforcement agencies. Here again, differing legal regimes complicate the issue. In some countries, for example, ISPs and other telecommunications companies are required by law to destroy transactional data -- data that may be crucial to the identification and location of a cybercriminal.

The task for law enforcement, industry, and others is to identify solutions to these challenges - and to do so in a manner that respects privacy rights and civil liberties. Public confidence and support is essential to the success of the law enforcement community - - confidence that is undermined if the public believes we are unnecessarily infringing on the privacy rights we hold dear in this country. Moreover, law enforcement needs to focus additional attention on the intersection between high-tech crime and privacy. Many of the most egregious forms of high-tech crime - including cyberstalking, identity theft, and hacking cases - involve serious invasions of privacy. I believe the public expects us to protect privacy on both fronts - by respecting the constitutional and legal guarantees in the investigation and prosecution of crime **and** by vigorously enforcing laws designed to protect our privacy.

What We Are Doing to Combat Theft of Intellectual Property

Against this general background, I want to turn to what the Justice Department is doing to combat two forms of crime that are of particular interest to the high-tech industry -- theft of intellectual property and high-tech cargo theft.

Last July, I went to San Jose to announce the Intellectual Property Enforcement Initiative, a joint law enforcement initiative by the Justice Department, FBI, and Customs Service. The Business Software Alliance estimates that software piracy cost their industry more than $11 billion in lost revenue in 1998. These losses translate into lost jobs, lost taxes that would have been paid on the legitimate goods, less innovation, and higher costs for consumers.

But while the dollar losses to such crimes are staggering, they do not tell the full story. The substitution of counterfeit computer chips can pose a threat to the health and safety of the public, for example, where such chips are used in aircraft and have an increased possibility of failure. We likewise see threats to public health from counterfeit airplane parts, pharmaceuticals, and electrical parts.

In addressing these challenges, I am pleased to report that, in the six months since the Initiative was first announced, we have made substantial progress in every one of our goals.

First, enforcement efforts have increased in all seven of the geographic areas that we targeted -- including San Francisco and Silicon Valley, Los Angeles, Miami, Boston, New Jersey, New York, and Boston -- as well as in a number of other areas. Since July, Justice Department prosecutors have secured five convictions and brought charges against 11 other individuals in criminal intellectual property cases. I would like to share a few highlights:

- In the first conviction under the Initiative, prosecutors in the Central District of California (Los Angeles) charged a defendant with trafficking in more than **$13 million** in pirated software and music. Under a plea agreement, the defendant and his accomplice agreed to forfeit **387,000** counterfeit music and computer CDs and manufacturing equipment worth more than **$1.5 million**.

- In October, federal prosecutors in Miami charged several Florida corporations with conspiracy to smuggle and traffic in counterfeit computer components. The operation included equipment that was used to place counterfeit markings on central processing units (or CPUs) of high-end computers. The U.S. Attorney's Office in Florida also has charged a defendant and his company of trafficking in fraudulently branded baby food.

- In September 1999, in Manhattan **10** individuals were charged with operating a major counterfeit motion picture ring. In the investigation, agents seized more than **300** video cassette recorders and tens of thousands of video cassettes.

- Finally, two Districts have brought charges under the No Electronic Theft statute -- the so-called "NET Act." Enacted in late 1997, the NET Act makes it a criminal offense to distribute pirated software and other copyrighted materials, even if the defendant does not directly profit from the pirating activities. In the first-ever NET Act case, the U.S. Attorney's Office in Oregon obtained a felony guilty plea against University of Oregon college student who operated a website with the purpose of illegally distributing copyrighted software. And just last month, the U.S. Attorney's Office in Washington, DC, obtained a guilty plea in a second NET Act case. This case is particularly important because the plea agreement requires the defendant to use his website -- through which he previously distributed illegal software -- to warn others about the perils of illegal software distribution. This case received considerable attention in the computer press and, we hope, will have an important deterrent impact. The defendant's website can be found at "www.nopatience.com."

And there are more cases in the pipeline. The FBI reports that as of November 5, 1999, there are **455** intellectual property cases under investigation nationwide (including copyright, trademark, and trade secret matters). In fact, in the less than four months after the IP Initiative was announced in July, the FBI opened **110 new** IPR-related investigations.

Under the second prong of the Initiative, we have been working with industry to streamline and expedite the process by which companies bring IP violations to the attention of law enforcement. We have developed an "industry referral form" that identifies the key types of information we need to investigate and prosecute criminal IP cases. By providing law enforcement, at the earliest stages, with key information that goes to each element of the criminal IP statutes, we can streamline the referral process and use the limited resources of law enforcement and industry in the most effective manner possible.

Third, we are seeking increased penalties under the U.S. Sentencing Guidelines for criminal IP cases. Frankly, the current penalties are much too weak to provide an effective deterrent and do not adequately capture the serious nature of IP theft. The Justice Department has asked the Sentencing Commission to put this issue at the top of their agenda, and we are hopeful that the Sentencing Commission will issue a guideline amendment by May 1 of this year to increase criminal IP penalties. If your organizations wish to communicate their views on this critical subject, they may wish to respond to the Federal Register notice published in late December by the Commission, with a comment period that expires on January 26, 2000.

Fourth, we have bolstered specialized training for agents and prosecutors in IP cases. We have added new or expanded existing IP training courses for federal prosecutors, as well as for FBI agents and Customs Service officers. We also are working through our International Law Enforcement Academies in Budapest and Bangkok to step up international awareness and training.

And we are identifying other ways to boost awareness and enforcement efforts in the international arena. We are working with our trading partners to enact tough and effective criminal IP laws, and we are providing training to foreign law enforcement agencies on how to investigate and prosecute these cases. We are also working closely with the US Trade Representative, US Department of State, US Department of Commerce, and the Customs Service to integrate enforcement issues into the Administration's overall trade and foreign policies. We have raised these issues forcefully with the G-8 nations, and in one-on-one meetings with key foreign governments.

While we are making substantial progress in every component of the IP initiative, we believe we can and must do more to protect U.S. companies from the theft of intellectual property. In the future, I hope the number of U.S. Attorney's Offices formally participating in the IP Initiative will grow. To do this, we may need additional resources, and we will be working with Congress to identify how to provide these resources. We also may need to consider additional legislative proposals to promote IP enforcement efforts, and, here again, we will be working closely with Congress.

Cargo Theft

Before turning to suggestions on how we might work more effectively together, I would like to touch briefly on one additional area of concern to key segments of the high-tech industry -- cargo theft. Although the Information Age has spawned some new forms of criminal activity, the high-tech industry also is grappling with the old fashioned problem of theft of high-tech equipment. The extent of the problem is significant.

- According to recent statistics, theft of high-tech equipment will reach almost $10 billion in the next several years.

- In the last three years, insurance claims for high-tech thefts and robberies have increased by 600 percent. The Chubb insurance company reports that the average claim filed for high-tech theft rose from $5,000 in 1992 to $500,000 in 1995.

- In some areas, we are seeing violent gangs engaged in strong armed robberies involving computers and high-tech equipment. Intelligence indicates that some criminal groups are so sophisticated that they intentionally have put part-time or temporary employees to work in target companies, thus giving them inside information to plan and execute their robberies.

The extent of this problem is likely to grow in coming years. Some high-end computer chips are worth more than an ounce of cocaine. Millions of dollars of chips can be loaded into the trunk of an average car. The profits of high-tech theft can be as large as those from drug trafficking with significantly less risk because of the difficulty identifying the parts as stolen and the relatively low sentences for such crimes.

We have taken a number of steps to address these problems. First, the FBI has designated cargo theft as a priority enforcement area, and has launched an interstate enforcement effort directed at theft of high-tech equipment. Since most of these offenses also are violations of state laws, we are working closely with state and local agencies to share investigative information and intelligence and to ensure our resources are focused where they can be most effective. Finally, I would like to call your attention to the work of the Inter-Agency Commission on Crime and Security in U.S. Seaports, which was created by President Clinton last April. One of the specific mandates for the Seaport Commission is to examine the problem of crime at U.S. seaports, including cargo and high-tech theft. The Commission has scheduled three hearings around the country to gather information about the nature and extent of the problem and to formulate recommendations. The first hearing is in Norfolk, Virginia, in early February. I would encourage you to participate in these hearings, not only to emphasize your concerns, but also to offer constructive suggestions on what can be done to combat high-tech cargo theft.

Suggestions for Industry

This morning, I have outlined some of the challenges law enforcement is confronting in the Information Age. I discussed what we are doing in two key areas of interest to the high-tech industry: theft of intellectual property and theft of high-tech equipment. Now, I would like to conclude by offering some thoughts on what industry can do to assist us in combating high-tech crime and to invite your suggestions on how to improve our efforts.
While the Justice Department and our counterparts in the FBI, Customs Service and other federal, state and local agencies are working aggressively to combat high-tech crime, industry can and must play a significant role as well. Law enforcement, alone, will not be able to solve this problem. Ultimately, the answer lies in more effective efforts to prevent such crime, through effective internal security efforts, backed up by tough criminal enforcement efforts that provide a more effective deterrent and that appropriately punish criminal behavior once it occurs.

High-tech companies can take a number of important steps, some of which were discussed yesterday by David Goldstone from our Computer Crime and Intellectual Property Section.

First, we know that many forms of high-tech crime are committed by current or former employees. Rigorous personnel security practices, including background checks, can reduce the vulnerability in high-risk companies.

Second, internal policies and procedures can and should be implemented to assist in the early detection of losses. Strong inventory controls, for example, are essential because, if we cannot identify a product or prove that it was stolen, we cannot obtain a conviction. Companies also can take appropriate physical security measures, many of which can reduce losses and improve the safety of company personnel.

Third, industry can work more effectively with law enforcement. In some areas, such as intrusion cases, individual companies are reluctant to report such attacks due to concerns that their reputation will be harmed in the minds of investors, business partners, and the public. While this hesitation may be understandable, the collective effect is to hamper law enforcement's ability to combat high-tech crime. I believe we can develop mechanisms to allow companies to report such victims in a manner that does not expose such companies to an undue risk of negative publicity. We can also develop mechanisms for more effective referrals of potential violations of law.

Finally, I want to stress the need for more effective cooperative efforts. While I have outlined several suggestions for industry, I also recognize that you may have constructive suggestions for law enforcement. I encourage you to continue the dialogue we have established on these issues, with the goal of identifying concrete solutions to the problems we face.
For example, we are examining a number of areas where additional legislation may be necessary, including to address the jurisdictional challenges of cyberspace.

We welcome your thoughts and suggestions in this regard, as well as in other areas where you think we can be more effective.

Conclusion

In conclusion, I would like to thank you again for this invitation to discuss what we are doing to combat high-tech crime. While I am proud of our efforts, I want to emphasize that much work remains to be done by us all. We can be most effective when we all work together and so I would encourage you all to share with us the problems you have identified and the solutions you are considering. If we communicate in this manner we can insure that our efforts are coordinated and ultimately successful and also insure the continued growth of this vital part of our economy.

Thank you.