Day Two

Welcome and Keynote Address

Introduction of Keynote Speaker

The Honorable Sterling Johnson, Jr., *Judge, U.S. District Court, E.D. NY and Commissioner, U.S. Sentencing Commission*

Keynote Address

The Honorable Michael Vatis, *Director of the National Infrastructure Protection Center, Federal Bureau of Investigation*

INTRODUCTION OF KEYNOTE SPEAKER

PROFESSOR O'NEILL: We would like to welcome you to the second day of our Economic Crimes and New Technology Offenses Symposium. Today should prove to be an interesting day, in the sense that we are going to be focusing largely on technical crimes and the impact of the Internet and cyberspace on the sentencing guidelines and cybercrime.

I would like to make a couple of apologies in advance. First, I am not sure that Chair Murphy will be here this morning. Members of the Sentencing Commission were called to testify before the Senate Judiciary Committee in an oversight hearing. So we have the odd situation of having a symposium and also being called before the Judiciary Committee to testify in an oversight hearing. So we have a bit of a conflict here this morning.

I would also like to apologize in advance on behalf of FBI Director Freeh. Unfortunately, given the incidents of yesterday in the terrorist attack on the United States's naval vessel, Director Freeh has been called away this morning and will not be able to address us. But the FBI has sent a more than able replacement.

Obviously, our thoughts and our prayers go out to the families and the friends of those who were killed in that attack, and Director Freeh sends his best and hopes that we can excuse him at this time.

With that then, without any further adieu, I would like to turn the time over to my fellow commissioner, Sterling Johnson, who will provide the introduction to today's keynote speaker.

JUDGE JOHNSON: I received a call late last night, after the dinner, and was told that Director Freeh would not be here because of the terrorist attack in Yemen. He sends his apologies and a more than able replacement to take over for him.

Louis Freeh is a great guy. Mike, you tell him that we wish him well and our hearts go out to the men and women out there in Yemen.

Mike Vatis is the founding director of the NIPC, which is the National Infrastructure Protection Program, an interagency program that is designed to investigate and detect cyber attacks on our nation's infrastructure, including telecommunications, energy, banking, finance, transportation, and government operations.

The NIPC is located at the FBI and has been responsible for handling such incidents as the "Love Bug" virus, distributed denial of services attack on e-commerce sites, and the "Melissa" virus.

Mr. Vatis has been the director of NIPC since February of 1998. And from 1994 to 1998, he served at DOJ as the associate deputy attorney general and deputy director of the Executive Office for National Security. In this capacity, Mr. Vatis advised the AG and the deputy AG on information technology, high-tech crime, intelligence, counterterrorism, foreign policy, and national security issues and coordinated DOJ and national security activities.

From 1993 to 1994, Mr. Vatis served at DoD as special counsel in the Office of the General Counsel; and from 1990 to 1993, Mr. Vatis was engaged in private practice in Washington, D.C., concentrating on Supreme Court and appellate litigation.

Mr. Vatis served as a law clerk for the late Justice Thurgood Marshall, and from 1989 to 1990, he also was a law clerk to then Judge and now Justice Ruth Bader Ginsburg. She was on the Court of Appeals when he clerked for her.

Mr. Vatis graduated *magna cum laude* from Harvard Law School. At Harvard, Mr. Vatis earned a number of degrees including the Sears Prize in 1986 for the highest GPA in his class and served as supervising editor of *The Harvard Law Review.*

Mr. Vatis also graduated from Princeton University with a degree from the Woodrow Wilson School of Public and International Affairs. While at Princeton, he was a member of Phi Beta Kappa and the Varsity Heavyweight Crew Team. Mr. Mike Vatis.

KEYNOTE ADDRESS

MR. VATIS: Good morning, everyone.

I feel a little bit like Admiral Stockdale, who you may remember was Ross Perot's running mate in 1992, who had the immortal the line in a debate of "Who am I and why am I here?" But, hopefully, that intro gave you a little sense of who I am and why I might be an adequate substitute, hopefully, for Director Freeh.

I think the topic that you are discussing today and my remarks this morning are highly relevant to the two hallmarks of Louis Freeh's tenure as FBI director. One is the recognition that crime today is increasingly international in its scope. And I am not talking just about international terrorism or foreign counterintelligence, the two areas that have traditionally been international. I am also talking about organized crime, white collar crime, and, now especially, computer crimes.

All of these things are increasingly transcending national boundaries, and as a result, the FBI and other law enforcement agencies need to be prepared to address that internationalization of crime and be prepared to deal with our overseas counterparts. For that reason, Director Freeh has focused intensely on expanding the FBI's legal attache (LEGAT) program abroad—to have FBI agents located in American embassies in key countries around the world to facilitate our response to international crime that affects American interests abroad or that directly affects the American public here at home.

The other hallmark of Director Freeh's tenure has been trying to put the FBI on the cutting edge of technology so that it is capable of responding to high-tech crimes. That will be the focus of my remarks this morning. These two issues—internationalization of crime and the need for law enforcement to increase its technological capabilities—come together when we deal with Internet crimes and crimes that use computers as weapons because, obviously, the Internet knows no boundaries and, increasingly today, we are seeing that crimes involving the Internet have international aspects that cause us to rely on our LEGATs overseas in a tremendous way.

So both those hallmarks of Director Freeh's tenure are extremely relevant to what you will be discussing today.

I am very privileged to be here this morning with you to discuss computer crime and crime on the Internet. I have seen the work of the Sentencing Commission over the last decade—beginning with my work as a law clerk and then as a lawyer and an official at the Department of Justice—and I have great respect for the work that this Commission does to make equal justice under the law a reality rather than just a theoretical concept.

I believe that one of the most significant aspects of a truly democratic society is the manner in which it treats people who are found guilty of crime. Fortunately, our society is one founded on the notion that cruel and unusual punishment will not be tolerated and that punishment must be proportionate to the gravity of the offense committed.

I commend all of you for the hard work that you have done in the past and that you continue to do today, both in establishing what proper sentences should be and in informing key decision makers in the executive branch and in the legislative branch as well, as they consider these important matters.

I would like to focus today on what the FBI and the National Infrastructure Protection Center, in particular, are doing to protect the American public from the many new threats that are emanating from cyberspace.

Let me give you just a little background on the problem and convey why this is such an important area. The growth of the Internet has been tremendous. As of last year, there were over 100 million Internet users in the United States alone. And that number is projected to reach 177 million in the U.S. and 500 million worldwide by the end of 2003, so the growth pattern continues to be incredibly fast.

Electronic commerce, in the last couple of years, has also emerged as a very important sector of our economy, accounting for over $100 billion of sales in 1999, which was more than double the amount from the year before. By 2003, electronic commerce is projected to exceed $1 trillion.

But with this growth of e-commerce and usage of the Internet, in general, we have also seen a tremendous increase in the crime that has migrated to the Internet and the threats that emanate from those sorts of criminal activities.

Computers can, essentially, be used in two ways to commit crimes. First, they can be used to facilitate traditional sorts of crimes. The Internet can be used to engage in stock frauds and other sorts of fraudulent schemes on the Internet, with larger numbers of victims affected. It can be used to disseminate child pornography. And it can be used to convey extortionate threats.

But, second, the Internet and computers can also be used as weapons to commit new sorts of crimes, in which computers are used to attack other computers, either to steal information, to steal money, or to cause a "denial of service" of the computers themselves.

Foreign powers or economic competitors can penetrate a U.S. company's confidential system and steal its proprietary information or steal credit cards. Malicious hackers can get into a hospital database and alter the medical records of all the patients in the hospital.

And criminals can launch computer viruses or "distributed denial of service" attacks that can prevent the owners and operators of the computer networks from accessing the data on the computers or even using the basic services offered by those computers.

And, in the most significant or extreme scenarios, a terrorist group or foreign power can take hold of the computers that operate our nation's critical infrastructures: our electrical power grids, our telecommunications networks and other services that are vital to our economy and to our national security.

The financial costs of these sorts of attacks are very high. According to the most recent survey conducted by the Computer Security Institute and the FBI, 273 respondent companies reported a combined loss of $265 million for that year alone, for 1999 alone, which averages to almost $1 million per company.

In order to deal with this problem, the FBI is conducting an unprecedented outreach program to the private sector, because it is, after all, the private sector that is the primary victim of these sorts of attacks and that owns and operates our nation's critical infrastructures.

One program, in particular, is called InfraGard which refers to guarding our infrastructure. This is an initiative that actually began with private companies in Ohio that wanted to reach out to the FBI and engage in a dialogue about how to deal better with some of these threats that I have been talking about.

One vital component of InfraGard—which is now a nationwide program that is based around FBI field offices in 56 cities—is the ability of industry to report to the local FBI field office and to the NIPC back in Washington information about an incident or a threat that they have experienced. They can do this in a sanitized format that protects the company's identity, and they can do it in a detailed format that allows for an immediate investigation of the incident.

But the decision whether to report, and the substance of the report, are left up to the company. The company decides what information it wants to provide and what it is willing to allow us to do with the information; and then we, in turn, can launch an investigation of the incident and also use the information to see if there are broader trends. We can look at the information in conjunction with other information we get from investigations, from intelligence data, from open sources, and then we can put warnings out to other people in the private sector so that they can protect themselves from similar attacks.

One thing we have seen over the last couple of years is that there are very few isolated incidents. Each incident seems to have a corresponding incident in another city, with another company. So there are a lot of trends that we see that need to get out there into the public eye so that people can protect themselves.

Another effort we have underway is something called our Key Asset Initiative (KAI), which is an attempt to determine which infrastructures are truly critical to our nation's economy and national security. Where are the hard assets that compose those infrastructures, and what can we do to work with the owners of those assets to protect them from cyberattack?

This was a program that actually started in the 1980s and was focused on protecting against the sort of terrorist attacks through physical means that we saw in the 80s and 90s. But now, with the tremendous growth of the Internet and the possibility of cyberterrorism and cyberattack on these infrastructures, we have broadened the focus of the KAI to include looking at vulnerabilities to cyberattack and are, again, working with the owners of these key assets to protect them against those sorts of attacks, as well.

Our central philosophy in dealing with cybercrime is that the business community and the public will continue to expect that the FBI will offer the same level of protection against technology crimes that it tries to offer against physical crimes. Our philosophy is that technology should not make us more vulnerable to criminal behavior and that we, therefore, need to develop and maintain the technical capability that will allow us to provide the services that the public expects from us.

At the same time, the FBI and society in general, I think, understand that the balance between law enforcement's need to investigate crimes, on the one hand, has to be balanced against citizens' right to privacy, on the other. That is a balance that was struck in the Fourth Amendment to the Constitution and is also present in many federal statutes that attempt to define when and how law enforcement can get certain types of orders that allow us to invade people's privacy for the purpose of protecting public safety and investigating crimes.

We cannot, however, allow technology to outstrip the law and to upset the balance that the founders considered and implemented through the Fourth Amendment, and that subsequent Congresses have also implemented in statute. We have to ensure that the technology serves our goals and our values, rather than making us slaves to the technology.

Now some laws might need to be changed in order to ensure that we continue the balance that we have already struck and to update them to make sure that they are technology-neutral and that they don't impede the growth of technology. But we also have to ensure that the new laws don't upset that balance.

Officials from the Department of Justice and the FBI have testified about some of the recent bills that have been put before Congress, and there is a lot more information on the DOJ website and on the FBI website about those particular laws.

There have also been some bills that have been proposed that I think would go too far in regulating what law enforcement can do on the Internet and that, in fact, impose more restrictions than are present in the physical world. These, I think, would unduly impede our efforts to make sure that we are capable of dealing with technology crime.

Again, the Justice Department's testimony can be found on the DOJ website, and I think it offers some guidance to policy makers, like many of you, who are beginning to consider some of these crucial issues. So I would highly urge you to read some of the testimony by DOJ and FBI officials.

On the international front, which I mentioned at the outset, we have realized that fighting computer crime and Internet crime cannot be done exclusively within the U.S. Because telecommunications and the Internet are truly global, cyber criminals have the ability to act globally, and we must be able to do so as well.

As a result, as I said at the beginning, the FBI has reached out in unprecedented fashion to our counterparts overseas, and we have had many examples just in the last two years of extensive cooperation between the FBI and the Royal Canadian Mounted Police in Canada, New Scotland Yard in the U.K, and many other foreign law enforcement agencies. I will give some examples of those in a moment.

Again, as I mentioned, the LEGAT program has now been expanded to 40 legal attaches in embassies around the world, with the prospect of a greater expansion this year and next, because we are finding that, with crime spreading in such an unprecedented fashion, we need to have on-the-ground presence in a vastly increased number of countries around the world.

What exactly is the FBI doing in this area? Well, you have heard a little bit about the NIPC. Let me just mention a couple of other things that we are doing in the NIPC, in addition to having the NIPC at FBI headquarters. We have also created a program in all FBI field offices that places at least one agent in each of the FBI's 56 field offices who is capable of responding to computer crimes.

Sixteen of those field offices have full squads of agents who are capable of robust response to some of the most technical and complicated investigations that we have ever seen. Clearly, we have to expand our presence in the field offices if we are to keep up with the huge growth in cybercrime because computer crime is not limited to just the largest cities in the U.S. It can also be found in the smallest communities across the country, so we need to make sure that we have the ability to respond across the country quickly and with great technical competence.

We also, through the NIPC, regularly issue warnings, through a variety of mechanisms, to the private sector and to other government agencies. We do this through the InfraGard program, through our websites, and through a variety of other electronic mechanisms. And we also publish on our website analyses of virus and hacker trends, as well as of system vulnerabilities, so that people can stay alert to what the latest hacker trends are and protect themselves against some of the exploits that we are seeing.

On a separate note, the FBI has also recently set up, in conjunction with the National White Collar Crime Center, something called the Internet Fraud Complaint Center. This was set up in May of this year to combat and centralize reporting of fraud on the Internet—not intrusions and viruses, but fraud schemes on the Internet which were also growing at a tremendous pace.

We have had a lot of success in dealing with this problem. As the trend of computer crime has increased, we have also seen a great increase in the number of our pending cases. Let me just give you a couple of numbers on that.

In September '98, we had 601 cases involving computer intrusions, viruses, and denial of service attacks. A year after that, in September of '99, that number had grown to 801. Currently, we have nearly 1,200 open cases involving intrusions and viruses and denials of service (and not including Internet fraud).

So the numbers are growing very quickly. But it should be kept in mind that these are incredibly complex cases, which often require very lengthy and time-consuming investigations before an arrest is made.

Let me give you a few examples of some of the cases, just over the last two years, that the FBI and other agencies have worked on to give you a sense of the complexity of the cases, the international aspects, and also, some of the harm that can be caused in these cases.

In August of this year, as you may have read about in the papers, two suspects from Kazakhstan were arrested in London for breaking into the computer networks of Bloomberg, LP, and attempting to extort the company. The suspects demanded that Bloomberg deposit $200,000 into an account at Deutsche Bank in London. The case was investigated by the FBI, working closely with the London Metropolitan Police and the authorities in Kazakhstan as well.

With the cooperation of those agencies and with excellent cooperation from Bloomberg— including the CEO, himself, Michael Bloomberg—the suspects were taken into custody in London and are now being sought for extradition to the U.S. by the Department of Justice. That is just one case of a rising trend we are seeing of people breaking into computers for the purpose of then extorting the owner of the computer system.

Another case from this year involved a computer hacker who went by the name of Curador, who allegedly compromised e-commerce websites in the U.S., Canada, Thailand, Japan and the United Kingdom and stole as many as 26,000 credit cards from those sites. Many of those credit card numbers were then posted to various Internet websites for downloading by people who wanted to use those numbers to get free services or goods.

Curador gave an interview to the Internet News Service in which he reportedly stated that, "Law enforcement couldn't hack their way out of a wet paper bag. They are people who get paid to do nothing. They never actually catch anybody."

Two weeks later, after an extensive international investigation by the FBI and a local Welsh police service in a town called Dyfyd Powys, Curador was arrested at his residence. Curador is 18 years old and was arrested with another co-conspirator under United Kingdom law where both are being treated as adults, and the damage estimates in that case are still being determined.

Another case, which probably affected many of you last year, involved the "Melissa" macro virus, which was at the time one of the most significant and fast-spreading viruses the world had ever seen. It was a macro virus that spread when a user opened a Microsoft Word file attached to an e-mail. The virus did not destroy or alter data directly, but quickly generated a huge volume of e-mail which placed a significant burden on the networks on which the virus was found and shut down many e-mail servers.

The organizations that were affected incurred tremendous losses in productivity and e-mail traffic while they tried to purge the infected messages and rid their systems of the virus. The "Melissa" virus was a good example of the NIPC working both sides of its mission: issuing warnings to people to try to raise public attention so that people wouldn't open infected e-mail attachments, and also facilitating an investigation by FBI field offices in conjunction with state and local police.

Ultimately, America Online provided a significant tip to the New Jersey State Police, and their follow-up investigation with the FBI's Newark Division, the U.S. Attorney's office in New Jersey, and the Department of Justice led to the arrest in April of last year of the propagator of the "Melissa" virus.

That person, David Smith, ultimately pled guilty to one count of violating 18 U.S.C. § 1030 and to four state felony counts as well. In his plea, he stipulated to affecting at least one million computer systems and causing $80 million in damages. Many experts believe that the actual damage was probably ten times that amount.

Two other examples are very significant: one, earlier this year in May, was the "I Love You" virus which dwarfed the "Melissa" virus by comparison. I probably don't need to go into great detail about that because many of you were affected by it, no doubt, and I am sure you followed the course of the investigation in the newspapers.

But that was, again, a very fast-spreading virus which raced around the globe, literally, in a couple of hours and shut down e-mail servers and degraded the operation of computer networks at very significant private sector companies and government agencies as well.

The FBI was able to trace that virus in less than 24 hours to the Philippines and worked very closely with the Philippine National Bureau of Investigation to identify a suspect. Many of you have also heard that charges have been dismissed in the Philippines because the Philippines lacked a specific computer crime law.

That, I think, is a good example of some of the difficulties that we face internationally. But the case was significant in demonstrating the capabilities that law enforcement has acquired in the last several years and our improved ability to respond quickly to these sorts of incidents.

The final example was the "distributed denial of service" attacks in February of this year. The possibility of a distributed denial of service attack was actually something that we learned about a year ago, last Fall. Essentially, a distributed denial of service (or a "DDOS") attack involves a hacker taking over the networks of dozens or even hundreds of entities, often universities or private companies that have a lot of bandwidth.

The hacker then can place malicious code on all of those networks which allows him basically to take those networks over, direct them against his ultimate target, and flood that target with false communications, essentially shutting that target down.

We issued warnings about the threat of DDOS attacks last year, but the problem is that there really is no way to completely prevent these sorts of attacks from happening. Security against DDOS attacks actually depends on a community-wide effort by universities and companies to make sure that they are not infiltrated by a hacker and then used to attack someone else.

In addition to issuing warnings, we actually developed software that people could use to scan their systems to see if they had been taken over by a hacker, and we made that available on our website in December of last year. Several thousand companies used that software and actually found that they had been victimized by a hacker and had malicious code on their systems, and they were able to clean up their networks.

But, given the growth of the Internet, obviously, there are a lot more places out there that could be victimized and that were victimized. In February of this year, we saw an array of e-commerce sites and online news sites brought down by a DDOS attack.

Now, again within several days, the FBI was able to trace many of these attacks to Canada and worked closely thereafter with the Royal Canadian Mounted Police. Ultimately, within a couple of weeks, they identified a house in Canada that some of the hacks that then led to the DDOS attacks seemed to emanate from.

Earlier this year, an individual was arrested in Canada and charged with many of those attacks. The individual was a juvenile who went by the name "Mafiaboy."

So these examples, I think, convey a sense of the complexity of these sorts of cases, of the internationalization of computer crime, and also of the tremendous damage that can be caused by one fast-spreading virus or one set of denial of service attacks, and of the financial damage that can come from the theft of credit cards or the theft of proprietary information.

We have made tremendous progress, over the last three years, in dealing with these types of cases, by improving the technical capacity of our agents and improving our ability to work with other agencies and with the business community. But we also, clearly, have a long way to go to make sure that we can keep up with the fast growth of this problem and keep ourselves at the cutting edge, so that we are not playing catch up with the bad guys but, in fact, can stay a step ahead of them.

I appreciate the opportunity to be here, again. At this point, if I have time, I would like to take any questions you might have.

QUESTIONER: What are you actually doing in terms of special efforts in recruitment of specially trained experts, especially regarding juveniles who are committing computer crimes?

MR. VATIS: The question was whether we are doing any special recruiting in order to ensure that we can have the technical capability to keep up with the bad guys. There was also the suggestion that a lot of these cases involve teenagers.

Let me just, first, deal with the premise. A lot of these cases do involve teenagers. But, in fact, we have seen in recent years a large growth in the number of cases involving adults who are not just hacking for fun or to prove their skills, but are in fact engaged in malicious criminal activity with the motivation of illicit financial gain or of shutting down critical systems.

So it is not a problem just of teenagers. This is a very serious criminal area and also a national security threat, given the prospect of cyberterrorism or information warfare.

We are engaged in specialized recruiting. We have also done a tremendous amount of training for not only FBI agents, but also for agents in state and local law enforcement, since obviously federal law enforcement is just a small percentage of law enforcement in the United States as a whole.

To be totally frank, though, we are under pretty severe hiring constraints, simply because we have not seen a growth in the FBI's personnel level over the last couple of years and we are not slated to see any great future growth in the next couple of years. So we are really trying to train our existing work force because that is all that we have to work with currently.

We have made a lot of progress. And we are also trying to make sure that those agents that do have technical skills are being properly deployed and are not letting those skills lie dormant as they work bank robberies or other types of crimes. So, training is the number one thing we are trying to do, and, recruiting, once we have additional slots to fill, will follow.

QUESTIONER: Can you give us some idea what kind of punishment has been meted out, both here in this country and abroad when these offenders have been captured?

MR. VATIS: The punishment basically depends on the amount of damage that was done and the nature of the crime, whether it was something that was negligent, reckless or intentional.

Essentially, we are talking about five years for some of the most serious offenses. And, obviously, less than that for less serious offenses. I think if you look at some of the numbers and the damage that can be caused—millions if not billions of dollars of damage that can be caused by a virus or a hack—we need to look seriously about whether the sentences available are sufficient.

I think back when the Computer Fraud and Abuse Act was passed, a lot of people still thought of hacking as not really a tremendously serious form of crime. It was seen as often victimless, in some senses. But I think most people now realize that that is not the case, so I think we need to consider whether the existing penalties are adequate.

Overseas, the situation, if anything, is probably worse in that there are not a lot of significant penalties available in other countries. Even before we get to the penalty phase—I think as we saw with the

"I Love You" virus—in many countries there isn't even the substantive criminal law in place that allows for an investigation and prosecution.

So one of the things that we are doing through our international outreach efforts is try to encourage countries to pass substantive criminal law that allows for the prosecution of these sorts of cases, and then also to have adequate sentencing in place as well.

QUESTIONER: Could you just briefly explain how you figure out how much damage was done; you were referring to it earlier.

MR. VATIS: Figuring out damage can be very complicated. It depends on the type of incident you are dealing with. If it is an intrusion that resulted in the theft of information or the theft of money, it is relatively easy to put a value on what was stolen.

If it is a denial of service attack or a virus where nothing is stolen, you are usually looking at the loss of service of the network, the cost of repairing the network, the lost business opportunities, and things of that nature that require a lot of assistance from the victim companies in order to determine the amount of damage.

QUESTIONER: In the Director's testimony last March I think it was, he focused a great deal on intellectual property rights, even to the point of saying that violations of this type threaten the very basis of our economy. In the same testimony, he said they would be creating an IPR Center this year. My question to you is: has that center been created? Where is it? How does it function? And how does the private sector interact with that center?

MR. VATIS: I knew that I was going to regret taking one more question because I don't actually know what the precise status of the IPR Center is. As I mentioned, the Internet Fraud Complaint Center is up and running; obviously, the NPIC is. But I don't have a specific status report on the IPR Center, but I can get back to you, and I will take your card afterwards and get you that information. Perhaps someone here from the Department of Justice has that information.

MR. GREEN: I am David Green. I am deputy chief of the Computer Crime and Intellectual Property Section.

There is an IP Center that is jointly run by Customs and the FBI. It is housed at Customs. It is still getting geared up, but it will be gathering information, distributing information, analyzing information, and working with the private sector as well as with government agencies toward developing information about intellectual property crime.

MR. VATIS: Is there a place to call and a website already?

MR. GREEN: I don't think their website is yet up, but there will be something soon.

MR. VATIS: Thank you very much. Good luck.

PROFESSOR O'NEILL: I would like to thank you for that very interesting presentation. It kind of makes me glad that I had my early and budding days as a computer hacker back before the FBI got very sophisticated.