U.S. Department of Justice
Criminal Division
Office of the Deputy Assistant Attorney General
Washington, DC 20530

January 15, 2003

Deputy Assistant Attorney General Malcolm's Remarks Before the OECD-APEC Global Forum

January 15, 2003

I want to thank you for including me in this important discussion about the significant challenges of cybersecurity and cybercrime that face all of us.

I. Globalization of crime

New communications technologies, including advancements in electronic mail, wireless telephones, and the Internet, are the engine that will drive our developing worldwide information economy, and are already revolutionizing the way we conduct business, how we educate our citizens, and how we entertain ourselves during our leisure time.

These advancements, however, come with significant risks and responsibilities. From a law enforcement perspective, it is clear to me that our ability to successfully secure our networks will depend entirely on our ability to develop and implement a coordinated response to illegal activities that occur over those networks. This will require at least four tiers of action.

A. Legal Tools and Policies

The first tier is that governments must ensure that they have appropriate legal and procedural tools and practices in place to investigate and prosecute computer-related crimes. In addition to enacting suitable laws that criminalize and punish those who commit computer abuses and who engage in unauthorized access to computer systems, governments must commit adequate personnel and resources to fight cybercrime.

The need for technically-capable investigators who are dedicated to combatting high-tech crime is critical. Such experts must be available 24 hours a day 7, days a week, and must be supported with the best equipment available and be kept abreast of all changes in technology that might affect how cybercriminals do what they do. We are clearly no longer in an age where law enforcement agents can defeat criminals with a badge, a flashlight, and a gun.

When it comes to cybercrime, this new breed of villains requires new skills and tools for law enforcement. It is a new world, and law enforcement must be prepared to face the challenges posed by that new world.

Along that same vein, governments must improve their abilities to locate and identify criminals. Because of the speed and sophistication of cyberattacks and the ephemeral nature of the evidence left behind, law enforcment officials must get timely access to information and to traffic data without alerting the customer that such access is being provided. Procedural mechanisms must also be in place to preserve that data, in appropriate cases, for use in ongoing investigations and eventual prosecutions.

B. Coordination among components of government

Too often different components within government do not share vital information with each

other, and occasionally may even be working at cross purposes with one another. Hence, the second tier of action is that we must have better communication and more direct collaboration between different agencies and branches within government in order to advance the growth and improve the security of e-commerce.

As we work to amend government policies, rules, and regulations on a range of communications, technology and e-commerce issues to achieve better coordination and to advance the goals of effective law enforcment and enhanced publi safety, we must guard against unintended consequences, such as stifling the growth of the Internet or chilling open communication. We must do everything we can to ensure that, in our zeal to combat network crime, we do not needlessly sacrifice cherished civil liberties enjoyed by the citizens of our respective countries. This is a delicate balance that each of us will need to face.

C. Cooperation among governments

The third tier of action is that effective prosecution of illegal activities on our global network systems will require a coordinated response and cooperation among governments.

Because Internet access is available in over 200 countries and criminals can route their communications through any of these countries, the law enforcement challenges that we all face must be addressed on as broad a basis as possible.

It is critical that each of these countries enact sufficient laws to criminalize computer abuses and unauthorized access to computer systems. Where Country A criminalizes certain conduct and Country B does not, a bridge for cooperation may not exist. You will recall, for example, the "I Love You" virus that was released in 2000. In that case, the individual who released the virus was a Philippine citizen, a country which at that time did not criminalize unauthorized access to computers.

Fortunately, both the Council of Europe Cybercrime Convention and the U.N. General Assembly Resolution 55/63 constitute significant steps towards establishing a consensus among nations as to what acts ought to be criminalized.

While we must obviously respect the sovereignty of each other's countries, we must learn to work together to investigate cybercriminals who take advantage of the borderless nature of the Internet to commit and conceal their crimes. When it comes to combatting cybercrime that crosses borders, like a chain, we are only as strong as our weakest link. Happily, such efforts are already underway and are deserving of our attention in this ever-changing environment.

For example, the Council of Europe Cybercrime Convention provides a significant roadmap to ensuring that governments have well-developed and comprehensive legal and policy regimes for dealing with network crime. Similarly, the OECD Network Security Guidelines provide sound principles and guidance for online protection. There is also a growing network of high-tech points of contact in 30 nations (so far) that are available 24 hours a

day, 7 days a week to provide assistance to other countries on matters involving electronic evidence even in physical world crimes such as murder or kidnapping. This network was begun, and is administered, by the countries of the G8, but all countries with the necessary capacities have been urged to join.

D. Partnering with Industry

The fourth tier of action is that their must be a true partnership between government and the private sector when it comes to cybersecurity.

In the United States, for example, it has been estimated that roughly 85% of our critical infrastructure is controlled by the private sector. Clearly the private sector must play a leading role in assuring security and confidence in our shared networks, and governments must be prepared to work closely with industry at a variety of levels to respond to the problems associated with network security.

Not only does industry design, build and operate the infrastructure, systems, and related technologies that connect us, it has the know-how and resources to address these needs. Government, in turn, must take steps to protect its own computer systems, and to ensure that industry is not unnecessarily hindered in its efforts to secure network systems under their control.

In addition to developing a partnership based on trust and experience between government and the private sector when it comes to network security and law enforcement, we should also form a partnership to educate the public about computer security and to raise the level of awareness about computer responsibility – an area of so-called "cyberethics."

We must do a better job of educating the public about the risks of identity theft, theft of other personal and private infomation, and malicious worms and viruses from failing to take certain precautions. We must also do a better job of teaching people that hacking and copyright theft is not "good sport," but rather its wrong and causes real economic, and possibly physical, harm to others.

In this regard, the Department of Justice has supported President Bush's National Strategy to Secure Cyberspace and is actively reaching out to organizations and companies to focus national attention on cybersecurity and on advancing proper cyber-social behavior.

In conclusion, I note that many of the distinguished industry experts and government leaders who must play a role in meeting the challenges of cyber crime and in creating a culture of security are in this room. Although we often serve different societal interests, we meet here today with one common goal: to keep our countries' computer networks safe, secure and reliable for our citizens and businesses. I look forward to listening to your views and to working with each of you to make that goal a reality. Thank you.