Testimony of Deputy Assistant Attorney General John G. Malcolm on Cyberterrorism
Before the Senate Judiciary Committee
Subcommittee on Terrorism, Technology and Homeland Security
February 24, 2004

Good morning, Chairman Kyl, Senator Feinstein, and Members of the Subcommittee. On behalf of the Department of Justice, I would like to thank you for inviting me to appear before you this morning to discuss the important issue of cyberterrorism.

The Department of Justice's role in responding to cyberterrorism is shaped in large measure by the "President's National Strategy to Secure Cyberspace," which calls upon our entire society -- the federal government, state and local governments, the private sector, and the American people -- to engage in coordinated and focused efforts to secure cyberspace. Under the National Strategy, the Department of Justice and the FBI are charged with leading the national effort to investigate and prosecute cybercrime. Our role as law enforcement defines what it is that we do, namely, act to prevent and deter cybercrime; investigate cybercrime incidents; and identify and prosecute people who violate federal laws.

While we prevent and respond to cybercrime incidents, we do not do so in the same manner as the Department of Homeland Security ("DHS"). While DHS is responsible for identifying and protecting against "vulnerabilities" in the information infrastructure, we focus on responding to "threats" presented by intentional, unlawful acts that threaten the confidentiality, integrity, and availability of information networks.

I. Cyberterrorism – What is It?

Cyberterrorism involves the use of computer systems to carry out terrorist acts, which are, in turn, defined by reference to specific criminal statutes. True cyberterrorism is characterized by large-scale destruction (or the threat of such destruction) coupled with an intent to harm or coerce a civilian population or government.

There are many misconceptions about cyberterrorism. Not all cyberattacks are acts of cyberterrorism. In fact, the vast majority of network intrusions are committed by those who lack terroristic intent. Common examples of people who perpetrate cyberattacks, but who are not cyberterrorists would be so-called "script kiddies" who hack into computers for fun, sophisticated hackers who enjoy the challenge of exploiting security vulnerabilities, and disgruntled employees who seek revenge against their employers.

Even politically-motivated "hacktivists" who deface web sites in order to convey a political message will rarely qualify as cyberterrorists. For instance, the Department recently prosecuted an individual who hijacked the news agency Al Jazeera's web site, replacing it with his own political message. While these defacements can damage computer systems and networks, they do not usually cause the type of large-scale destruction that is implicit in cyberterrorism.

Attacks on critical infrastructure, on the other hand, have the potential for large scale disruptions and mass casualties, and may, depending on the motivation of the attacker, be linked to cyberterrorism. Examples of critical infrastructures include: telecommunications networks; transportation systems and services; water supply systems; energy systems; financial systems; and emergency services, including medical, police, fire, and rescue services. The issues of cyberterrorism and critical infrastructure protection ("CIP") are often intertwined for understandable reasons.

II. Cyberterrorism – What Has the Department of Justice Done to Prepare?

The Department is concerned about any unlawful computer intrusion, but most especially those that have the potential to affect critical infrastructure or which raise the specter of cyberterrorism. The motivation behind any particular cyberattack may not always be apparent at the outset of an investigation. For instance, in 1997, a juvenile hacked into the Bell Atlantic computer system, causing a system crash that knocked out power to the Worcester, Massachusetts airport. Ultimately, it was determined that the individual lacked terroristic intent, but the hack was nonetheless criminal and potentially life-threatening.

In light of the uncertainty regarding motive, prudence dictates that we respond to all cyberattacks in the same manner. After all, if the attack in question can be perpetrated by an ordinary criminal, it can certainly be perpetrated by a cyberterrorist. While we have been fortunate enough not yet to experience a devastating act of cyberterrorism or a crippling attack

on a critical infrastructure, the hard lessons of 9/11 teach us that preparation is critical.

Domestic Efforts

A. CCIPS

The Department has developed specialized expertise in the area of cybercrime. The Computer Crime and Intellectual Property Section ("CCIPS"), which I oversee, has a team of 37 attorneys who focus exclusively on issues relating to computer and intellectual property crime, and who respond daily to requests for information and advice from the 94 U.S. Attorneys' Offices across the nation. In addition, the Section coordinates multi-district cases and engages in important education and outreach efforts, providing hundreds of hours of training each year to prosecutors, agents, judges, technical experts, and government and industry groups. CCIPS has also published significant reference manuals for prosecutors, including one on *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*.

B. CTC Network

Another important component of the prosecutorial framework is the network of Assistant United States Attorneys who have been designated Computer and Telecommunications Coordinators ("CTCs"). Each district has at least one CTC (there are a total of 212 CTCs) who receives special training from CCIPS so that he or she can function effectively as a resource for

their district and as a point of contact for multi-district cases. Recent training sessions have emphasized the prosecutor's role in critical infrastructure protection and the importance of fostering communications with our military counterparts, including the Joint Task Force Global Network Operations (JTFGNO).

C. CHIP Units

There are also a total of thirteen Computer Hacking and Intellectual Property ("CHIP") Units comprised of specially-trained personnel, including prosecutors. The location of these specialized units was based on a number of factors, including their proximity to high-tech industry areas, their potential for growth in that area, and the presence of adequate FBI resources to investigate these crimes. In addition to prosecuting cases, the CHIP units focus on the prevention of cybercrime by working with local industry to anticipate future trends, identify vulnerabilities, and stop cybercrime before it occurs.

D. Partnerships

The Department has focused not only on developing internal expertise, but also on developing partnerships with other federal agencies, with state and local law enforcement, and with industry organizations. We work particularly closely with DHS's National Cyber Security Division ("NCSD") so that it can fulfill its mission of analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure

information systems. In turn, NCSD supports the Justice Department's mission of investigating and prosecuting threats and attacks against cyberspace. The Department also works with DHS as part of the Cyber Interagency Incident Management Group ("Cyber IIMG"), which develops response plans so that federal agencies will be prepared to respond in the event of a cyberterrorist attack or other cyber crisis.

At the state and local level, the Department participates on the National White Collar Crime Center's Cybercrime Advisory Board, which provides recommendations on issues of cybercrime collaboration among law enforcement, academia, and the private sector. The National White Collar Crime Center is a non-profit organization funded by Congress that provides support services to state and local law enforcement agencies and other organizations with an active interest in the prevention, investigation, and prosecution of economic and high-tech crime.

The Department has also worked with the National Association of Attorneys General ("NAAG") to compile the Computer Crime Point-of-Contact List, a 50-state list of state and local prosecutors and investigators who are responsible for computer-related crimes within their respective jurisdictions. This list allows agents and prosecutors from one jurisdiction to call upon their colleagues in another jurisdiction for rapid response in cybercrime matters.

We have also developed productive relationships with business and industry organizations. The Department has supported the FBI and the National Infrastructure Protection

Center ("NIPC") in developing the "InfraGard" initiative, which expands direct contacts between government and private sector infrastructure owners and operators and encourages the sharing of information about computer intrusions, vulnerabilities, and infrastructure threats. Since the NIPC became part of DHS, the Department has continued to engage in regular outreach through InfraGard to ensure that communication channels are open between government and the private sector.

International Efforts

Because cyberattacks frequently transcend geographic boundaries, the Department's cybercrime initiatives have not been confined to the United States. It is vitally important to have foreign counterparts who are technologically capable, who are accessible and responsive, and who have the necessary legal authority to cooperate with us and assist in our investigations and prosecutions in the event of a trans-border cyber incident.

A. G8 Subgroup on High-Tech Crime: 24/7 Network

We are working hard to build strong relationships with foreign counterparts so that the framework will be in place to quickly respond to cybercrimes, including large-scale cyber incidents. For example, CCIPS chairs (and has chaired since its inception in 1997) the G8 Subgroup on High-tech Crime. One of the most significant achievements of this Subgroup is the creation of the "24/7 Network," which allows law enforcement in the participating countries to

reach out – 24 hours a day, 7 days a week – to counterparts in other countries for rapid assistance in investigating computer crime and preserving electronic evidence. Often, cyber-criminals can be identified only if evidence of their conduct is preserved within minutes, a time-frame that is way too short for us to rely on traditional international assistance options.

Currently, 35 countries participate in the 24/7 Network. This network has been used successfully in many instances to investigate threats and other crimes in a number of countries, including the United States. Because terrorists operate throughout the world, it is critical that we continue our efforts to expand the Network in order to ensure that our law enforcement capabilities are coextensive. When it comes to combating cybercrime across international boundaries, the chain is truly only as strong as its weakest link.

B. OAS

The Department is active on several committees of the Organization of American States ("OAS") that relate to cybersecurity. OAS is the regional governmental organization for nations in North, Central and South America and the Caribbean. A senior attorney from CCIPS chairs the OAS Group of Government Experts on Cybercrime, and a CCIPS delegation recently traveled to Mexico to conduct training on drafting cybercrime laws for legislators, senior policy makers, and law enforcement officials.

C. APEC

We have worked with other regional governmental groups, including the Asia Pacific Economic Cooperation Forum ("APEC"), on issues relating to cybercrime. Specifically, CCIPS has been involved with APEC's Telecommunication and Information Working Group, which has sought to strengthen the capacity of institutions through the Cybercrime Legislation and Enforcement Capacity Building Project and the Computer Emergency Response Team Awareness Raising and Capacity Building Project. During the past year, CCIPS attorneys traveled to Thailand to conduct training on drafting cybercrime legislation.

We intend to continue our work towards improving the quality of cybercrime legislation and response mechanisms in other regions of the world. Much of our international work requires the cooperation of other federal agencies, such as the State Department's Office of International Narcotics and Law Enforcement Affairs, which has provided funding for developing international cybercrime enforcement capacity. We believe that improved laws will not only serve as a deterrent, but will also increase the overall prosecution of cybercriminals, including cyberterrorists, who would seek to operate in otherwise lawless nations.

III. What Legal Tools Are Available to Respond to Cyberterrorism?

A. Substantive Laws

There are a number of criminal statutes that might apply to a given cyberattack depending on the circumstances. For instance, the Computer Fraud and Abuse Act (18 U.S.C. § 1030) prohibits, among other things, unlawfully accessing classified information; obtaining information without authorization from a government computer or federal agency; and causing damage to a protected computer that results in physical injury, a threat to public health or safety, or damage to a computer system used for purposes of national defense or national security. The Department has prosecuted numerous cases under § 1030, including:

- a January 2004 conviction of a hacker who damaged computer systems belonging to eBay and Qualcomm using a Trojan program that allowed him to obtain user names and passwords;
- another January 2004 conviction of a hacker who illegally accessed the New York Times's internal computer network, including a database containing information and social security numbers for 3,000 individuals; and
- the arrest in August and September 2003 of two individuals charged with distributing variants of the Blaster computer worm.

Specific terrorism statutes might also apply in the event of a cyberattack. For instance, 18 U.S.C. § 2332b criminalizes acts of terrorism that transcend national boundaries. Other statutes might apply to domestic cyberterrorism. In one case in which an individual claimed to have electronic evidence of a missile threat targeting the opening ceremonies of the 2002 Olympic Games in Salt Lake City, which turned out to be a hoax, the individual was charged

under 18 U.S.C. § 844 for making false threats regarding explosives.

Penalties for acts of cyberterrorism are great. Under the Homeland Security Act of 2002, cyberattacks that result in serious bodily injury are punishable by up to 20 years in prison. If the attack results in death, punishment may be up to life imprisonment. The U.S. Sentencing Guidelines were also modified recently to provide for an upward departure in cases where the disruption to critical infrastructure resulted in a debilitating impact on national security, economic security, public health or safety.

B. Procedural Laws

In addition to substantive laws, the Department relies to a large extent on procedural laws, which are particularly important in cybercrime cases because cyber-criminals are quite adept at covering their tracks and electronic evidence can be lost in a fraction of a second. I would like to take a moment to briefly describe the vital role that the USA PATRIOT Act plays in our CIP and cyberterrorism efforts.

Crucial provisions in the Act allow computer service providers to voluntarily disclose subscriber communications in the event of an emergency without fear of incurring civil liability. In one instance, high school officials cancelled classes and sent bomb-sniffing dogs through the school in response to an anonymous death threat posted to an Internet message board. The owner and operator of the message board initially resisted disclosing the evidence on his

computer that could be used to identify the threat-maker because he had been told that he would be liable if he volunteered anything to the government. Once the message board owner/operator understood that the USA PATRIOT Act had created an emergency provision allowing the voluntary release of information, he disclosed evidence that led to the timely arrest of a student at the high school. The student ultimately confessed to making the threat. The message board owner/operator stated that he had been worried for the safety of the students and teachers at the high school and was relieved that he was able to help because of the change in the law.

Another invaluable provision in the USA PATRIOT Act permits courts to issue nationwide search warrants for electronic communications. This provision has relieved the heavy administrative burden for prosecutors and judges in the districts that are home to the large Internet service providers. More importantly, the efficiency has preserved time-sensitive evidence in cases in which the evidence might otherwise have been lost, such as one involving the tracking of a fugitive and another involving the theft of trade secrets. Such procedural means of obtaining expedited access to electronic communications will undoubtedly be crucial in the event of a cyberterrorist incident.

I could talk at length about the importance of the USA PATRIOT Act, but in the interest of time, I will keep my remarks brief. You are no doubt aware that many of the USA PATRIOT Act's provisions are currently set to expire. Because the Department has relied on these provisions in numerous instances to conduct successful prosecutions, and because these provisions would be essential to any prosecution for cyberterrorism, I urge you to not allow these

provisions to sunset.

V. Conclusion

As you can see, we are working on multiple fronts – both domestic and international – to address cyberterrorism and attacks on critical infrastructure. Our many efforts are intended to strengthen the communication systems necessary to ensure that cybercrime is successfully prosecuted. Thus, we have focused on building relationships with state and local law enforcement, with business and industry, with other federal agencies, and with our foreign counterparts so that we can move quickly to respond to cyberattacks of any sort.

While I would like nothing better than to be able to assure you that an act of cyberterrorism will never occur, unfortunately, I cannot do that. I can, however, assure you that the Department is taking – and will continue to take – the necessary steps to prepare to respond appropriately in the event of a cyberterrorist attack.

I thank you again for allowing me the time to address the Subcommittee on this very important issue. I would be happy to answer any questions that you may have.