Statement of

The Honorable Patrick Leahy

United States Senator
Vermont
February 24, 2004

Statement of Senator Patrick Leahy,
Ranking Member, Senate Judiciary Committee
Hearing On
"Virtual Threat, Real Terror: Cyberterrorism in the 21st Century"
February 24, 2004

Today's hearing will examine issues related to the potential misuse of computer technologies to commit terrorist acts.

As Senator Kennedy noted recently in connection with the Republican staff spying and stealing of internal Democratic computer files from the Judiciary Committee computer server, to gain access to sensitive materials it is no longer necessary to act under cover of night, or even to be physically present, as in the Watergate days. We must acknowledge and respond to the threat that devastating terrorist attacks can be launched by breaking into our most sensitive systems from across the globe. Such a cyber attack could cause immense disruption to our energy grid, water distribution systems, financial markets, and medical services. Our ability to thwart these attacks is critical to our protection of the nation's critical infrastructure.

As co-chair of the Congressional Internet Caucus, I have long supported efforts to secure Internet use. Last year, Senator Burns and I worked hard to ensure that tough criminal penalties were added to the CAN-SPAM Act, which among other things, penalized the use of spam to disable networks. In addition, last year I supported the Government Network Security Act, which helps to protect our government computers from the dangers of certain kinds of peer-to-peer software. A few years ago, I joined with Senator DeWine to pass the Computer Crime Enforcement Act, which authorized a grant program to help States prevent and prosecute computer crime. In the 104th Congress, I joined with Senators Kyl and Grassley to enact the National Information Infrastructure Protection Act to increase protection under federal law for both government and private computers and to address the problem of computer-age blackmail in which a criminal threatens to harm or shut down a computer system unless extortionate demands are met. In the 103rd Congress, I authored the Computer Abuse Amendments Act of 1994, which was included as part of the Violent Crime Control and Law Enforcement Act signed by President Clinton. Back in 1986, I sponsored the Electronic Communications Privacy Act, which outlawed tampering with electronic mail systems and remote data processing systems. In 1984, I worked to pass the Computer Fraud and Abuse Act to criminalize conduct carried out by means of unauthorized access to a computer. These are matters on which I have worked and about which I have cared deeply for more than two decades.

While to this point we have been fortunate that terrorists have not been able to infiltrate and dismantle our networks, we can assume, unfortunately, that they would if they had the opportunity. Recent reports about domestic uses of worms and other computer viruses also remind us that our vulnerability is not limited to foreign threats.

The Internet connects government computers with the private sector. It connects computers on the other side of the globe with ones responsible for monitoring our most sensitive functions, like commercial air traffic control. And it connects us all to one another in a way that makes commerce and government more efficient than ever before. While this has brought us benefits, it has also meant that our vulnerabilities are dispersed more broadly, as well.

It is essential that we work with the private sector to thoroughly assess our weaknesses and take steps to deal with them. It is also critical that we work with our world-class university system, which has developed innovative ways to protect our critical infrastructure. For example, the National Center for Counterterrorism and Cybercrime at Norwich University in my home state of Vermont has come up with cutting-edge approaches to fend off computer attacks and determine the vulnerability level of key systems.

We must ensure that appropriate levels of security and safeguards are in place to prevent abuse and to protect public health and safety. Unfortunately, the Administration has taken a step backward in its promulgation of an interim rule on so-called critical infrastructure information. This rule provides an overly broad exemption from the Freedom of Information Act to virtually any information that private companies voluntarily submit to the Department of Homeland Security. Along with Senator Bennett and Senator Levin, I had worked out a more balanced proposal when the legislation was considered in the Senate. That language is now embodied in the Restore FOIA Act, S.609.

I welcome today's hearing. I look forward to learning more about the Government's assessments of its abilities to prevent cyber terrorism and those of other experts.

And on a personal note, we have seen recent reports that John Malcolm will soon be leaving his post at the Department of Justice to fight piracy for the Motion Picture Association of America. I wish him well in that endeavor.

# # # # #