

**Comments of the United States Internet Service Provider Association
On Section 225 of the Homeland Security Act of 2002
Sentencing Guidelines
March 17, 2003**

The United States Internet Service Providers Association (US ISPA) is an organization comprised of major Internet Service Providers (AOL Inc., Cable & Wireless, eBay, EarthLink, Microsoft, SBC Communications, Teleglobe, Verizon Online, WorldCom, and Yahoo) throughout the United States. US ISPA welcomes this opportunity to submit written comments to the U.S. Sentencing Commission regarding Section 225 of the Homeland Security Act of 2002, sentencing guidelines applicable to defendants convicted of violations under the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. §1030.

Computer crime, including virus creation and distribution, computer intrusions, denial of service attacks, and theft of personal information, has continued to steadily increase over the last decade. Recent congressional testimony given by Assistant Attorney General Michael Chertoff, head of the Criminal Division at the Department of Justice, indicated that "there is no doubt that the number of crimes involving computers and the Internet is rising dramatically." For example, the CERT Coordination Center, which was created to warn network operators about computer attacks and viruses, received over 21,000 network crime incident reports last year. This is more than double the number of reports it received the previous year. Similarly, a survey conducted by the FBI and the Computer Security Institute recently revealed substantial increases in computer crime. Over 85 percent of the companies and government agencies surveyed reported computer security breaches within the preceding twelve months, up from 70 percent last year. Moreover, researchers at the University of California at San Diego recently reported a methodology that enabled them to count the numbers of denial of service attacks on the Internet; their research revealed that "4,000 attacks occur every week."

Some estimates of economic loss as a result of recent virus attacks add up to billions of dollars. Aside from the economic loss, our society's increasing dependence on computers means that the disruption of networks could seriously impair public safety, national security, and economic prosperity.

Today, however, sentences for violations of the CFAA are treated primarily as "white collar" fraud cases. Sentences are determined by calculating *actual or intended pecuniary harm*, something that is often difficult to quantify in the typical computer crime case. Under Guideline 2B1.1, significant economic loss is required before a defendant would even be eligible for imprisonment. In the case of the "Melissa" virus, a simple program that caused worldwide damage to millions of computers and computer systems, the perpetrator faced less than four years in prison even after proven damages of in excess of \$80 million. This lack of a significant criminal penalty eliminates the deterrent effect of a conviction, and makes the crime less likely to be prosecuted in the future. That is one reason that despite the enormous increase in the commission of computer crime, there is not a similarly large increase in prosecution of computer crime.

Newly emerging threats to the Internet, such as unsolicited bulk email, or spam, go largely unprosecuted because the type of harm spam causes is not currently addressed in the guidelines. Spammers send millions of unsolicited email messages that degrade and cripple entire email systems. However, the significant interference to the critical infrastructure caused by the abuse of spammers is not currently considered as a factor in the sentencing guidelines. Similarly, a common method for spammers to send bulk email, in an effort to by-pass spam blocking technology, is to steal personal email accounts and use their identities. The spammer's unauthorized access into the subscriber's account is a significant violation of the account holder's privacy rights. However, neither the violation of the individual's privacy rights by the spammer nor the spammers' financial gain from this illegal activity is taken into account in the sentencing guidelines, making prosecution for this type of offense extremely unattractive.

Moreover, the sentencing guidelines do not take into account the potential or actual harm caused by other types of crimes that may not cause economic loss, but have profound societal consequences: crimes that involve interference with important governmental functions, such as national security, national defense, and the administration of justice. For instance, viruses have attacked and taken down 911 operation centers in the past, knocking out the 911 emergency services for police stations and fire departments. This type of substantial harm to the public cannot be quantified in economic terms; and, if the perpetrators who created these viruses are finally caught, the disruptions they caused to these emergency services will probably not be used during their sentencing.

Cyber crimes should be viewed in the context of the overall incidence of the offenses and the extent to which they constitute a threat to civil peace and economic prosperity. The guidelines should not look just at the monetary damage a violation may cause, but at the important intangible loss of personal privacy and critical services that often results from cyber crime. Currently, the sentencing guidelines applicable to computer crime generally do not take into account these considerations.

We urge the Commission to amend the guidelines applicable to offenses under 18 U.S.C. §1030 to take full account of the eight factors listed in Section 225(b) of the Homeland Security Defense Act of 2002, particularly those factors that are not accounted for anywhere else in the applicable guidelines, such as whether the offense was committed for purposes of commercial advantage or private financial benefit; whether the defendant acted with malicious intent to cause harm in committing the offense; the extent to which the offense violated the privacy rights of individuals harmed; whether the offense involved a computer used by the government in furtherance of national defense, national security, or the administration of justice; whether the violation was intended to or had the effect of significantly interfering with or disrupting a critical infrastructure; and whether the violation was intended to or had the effect of creating a threat to public health or safety, or injury to any person. Economic loss alone does not adequately represent the threat to societal interests caused by computer crimes.