January 14, 2002

U.S. Department of Justice
United States Attorney
Eastern District of Virginia
Paul J. McNulty
2100 Jamieson Avenue
Alexandria, Virginia 22314
(703)299-3700
Fax: 703-549-5202

Cybercrime Initiatives Announced

United States Attorney Paul J. McNulty announced today the formation of one of the largest cybercrime units in the country, comprised of six Assistant United States Attorneys who will specialize in computer and intellectual property crimes. Attorney General John Ashcroft selected the Eastern District of Virginia to receive these additional resources to prosecute computer crime in this region as part of his "Computer Hacking and Intellectual Property" (CHIP) initiative. In making this announcement, Mr. McNulty was joined by Van Harp, Assistant Director-in-Charge, Federal Bureau of Investigation, Washington Field Office; Allen Doody, Special Agent-in-Charge, U.S. Customs Service; Peter Dowling, Special Agent-in-Charge, U.S. Secret Service; and Darryl Stilwell, Director, Bureau of Criminal Investigations, Virginia State Police. Computer crime or "cybercrime" has a significant impact on the Eastern District of Virginia because the backbone of the Internet is located here. Many Internet service providers, high technology companies, major universities, defense contractors, and federal agencies such as the Pentagon and Patent and Trademark Office which are located in this district are put at risk by electronic crimes. Even more troubling, cyber-terrorism threatens to disrupt the electronic systems of hospitals, utilities, banks, government, and other key institutions. "The protection of the integrity of the Internet, intellectual property, and our electronic infrastructures is one of my highest priorities," stated United States Attorney Paul J. McNulty. Fighting cybercrime is also a high priority for the Federal Bureau of Investigation, the U.S. Customs Service, the Secret Service, the Virginia State Police and other law enforcement agencies. The cybercrime unit will focus on a wide array of criminal activity including computer intrusions, denial of service attacks, virus and worm proliferation, electronic wiretapping, telecommunications fraud, political "hactivisim" (the use of computer crime to make political points), web vandalism or manipulation (sometimes called "semantic attacks" when targeting online news and information sites), Internet and computer fraud, theft of trade secrets and economic espionage, criminal copyright and trademark offenses, software piracy, and other forms of computer, Internet, and electronic crimes. The unit will also work closely with federal, state and local law enforcement, and industry to develop, coordinate, and implement effective strategies to combat these high tech crimes. In addition to prosecuting high-tech offenses, the cybercrime unit will develop regional training programs to increase expertise among federal, state and local law enforcement and will encourage those in the high-tech community to report computer crime and intellectual property offenses to law enforcement. United States Attorney Paul J. McNulty stated: "Our cybercrime unit is dedicated to fighting crime in this digital age. We must protect the citizens of this district from

sophisticated criminals who use new technologies to victimize society. There are no free passes in cyberspace. Crimes will be investigated and criminals will be prosecuted to the fullest extent of the law."

###