Statement of Steven M. Martinez
Deputy Assistant Director, Cyber Division
Federal Bureau of Investigation

Concerning Computer Provisions
of the USA Patriot Act

before the
Subcommittee on Crime, Terrorism, and Homeland Security
Committee on the Judiciary
U.S. House of Representatives

April 21, 2005

Good morning Mr. Chairman, Ranking Member Scott, and members of the subcommittee.

My name is Steven Martinez and I am the Deputy Assistant Director of the FBI's Cyber Division. The primary mission of the Cyber Division is to supervise the Bureau's investigation of federal violations in which computer systems, including the Internet, are exploited by terrorists, foreign government intelligence operatives, and criminals. In short, our mission is to protect the American public against a host of significant and potentially deadly high-tech crimes.

The uses of technology in our society are innumerable and their value immeasurable. The state of technology has been advancing rapidly over the past twenty years, much of it to the benefit of people living in all corners of the world. Unfortunately, the picture is not always so bright. Technology has also been used to harm people, while offering a particularly effective escape route. In this digital age, crimes can and do occur within seconds without the perpetrator ever getting anywhere physically close to the victim. In such a setting, law enforcement must be equipped with the investigative tools necessary to meet, locate, and incapacitate this growing threat. Law enforcement must be prepared to face sophisticated enemies and criminals who are known to exploit technology because of its ability to keep them far away from the scene of the crime, spread apart even from one another, and who have the ability to delete any digital evidence of their actions at the push of a button.

With this background in mind, I want to thank you for the opportunity to appear before you today to discuss certain sections of the USA PATRIOT Act which are scheduled to expire at the end of this year, specifically sections 209, 217, and 220.

When Attorney General Gonzales testified before the House Judiciary Committee on April 6, 2005, he shared his firm view that each of the provisions of the USA PATRIOT Act that are scheduled to sunset at the end of this year must be made permanent. Director Mueller provided the FBI's perspective in a hearing before the Senate Judiciary Committee on April 5, 2005, and he too

spoke of the crucial need to renew these provisions. Based on my knowledge of the interests, capabilities, and motives of those who, day in and day out, are attempting to do us harm by means of the Internet, I want to express my full agreement about the importance of the PATRIOT Act and the provisions I plan to address today. I believe that the Act's substantial merit can be demonstrated by what we already have experienced as a nation; still, it is equally true that the Act is essential so that we are prepared to confront the ever-evolving threat that no doubt will come.

SECTION 209 - SEIZURE OF VOICE MAIL WITH A SEARCH WARRANT

Going in numerical order, allow me to start with section 209. Section 209 permits law enforcement officers to seize voice mail with a search warrant rather than a surveillance, or Title III, order. Section 209 provides a very good example of how the USA PATRIOT Act simply updated the law to reflect recent technological developments. The drafters of the Act determined that obtaining voicemail stored on a third party's answering system is more similar to obtaining voicemail stored on a home answering machine (which requires a search warrant) than it is to monitoring somebody's telephone calls (which requires a TIII order). In passing this portion of the Act, Congress made the statutory framework technology-neutral. Privacy rights are still well accounted for, since section 209 allows investigators to apply for and receive a court-ordered search warrant to obtain voicemail pursuant to all of the pre-existing standards for the availability of search warrants, including a showing of probable cause. With privacy rights left firmly intact, there is a distinct advantage to the public's safety when law enforcement can obtain evidence in a manner that is quicker than the Title III process.

The importance of this provision is best understood in the context of how often terrorists and other criminals rely on technology to relay their plans to each other instead of risking face-to-face in-person meetings. Attorney General Gonzales gave a good sense of the diversity of those who would rely on the simple convenience of leaving voicemail in furtherance of their illegal activities when he pointed out that section 209 has already been relied upon to acquire messages left for domestic terrorists, foreign terrorists, and international drug smugglers.

Allowing section 209 to expire would once again lead to different treatment for voicemail messages stored on a third party's system than for the same message stored on a person's home answering machine. Doing so would needlessly hamper law enforcement efforts to investigate crimes.

SECTION 217 - THE HACKER TRESPASSER EXCEPTION

I would like to move next to section 217, the hacker trespasser exception. Like section 209 before it, section 217 also makes the law technology-neutral. Section 217 places cyber-trespassers -- those who are breaking into computers -- on the same footing as physical intruders. Section 217 allows the victims of computer-hacking crimes voluntarily to request law enforcement assistance in monitoring trespassers on their computers. Just as burglary victims have long been able to invite officers into their homes to catch the thieves, hacking victims can now allow law enforcement officers into their computers to catch cyber-intruders. Think for a moment how odd it would be if a homeowner yelled out to a police officer "Hey, there's a burglar in my house right now, help!", only to have the police respond, "Sorry, I have to apply for a court order first, try not

to scare him off." The homeowner would be dumbfounded, and the burglar would be long gone by time the police returned. This, in essence, is what was occurring prior to the PATRIOT Act.

It can be said that section 217, in a very significant way, enhances privacy. First, it is carefully crafted to ensure that law enforcement conducts monitoring against trespassers in a manner entirely consistent with protecting the privacy rights of law abiding citizens. Second, the essence of the section -- to help catch hackers -- serves a vital function in the FBI's ability to enforce data privacy laws.

With respect to the first point, the narrowly crafted scope of this legislation, section 217 preserves the privacy of law-abiding computer users by sharply limiting the circumstances under which the trespasser exception may be used. At its most fundamental level, section 217 requires consent. Law enforcement assistance is by invitation only. The computer crime victim is actually seeking the FBI's help. In addition, a law enforcement officer may not conduct monitoring based solely on the computer owner or operator's consent unless the law enforcement officer is engaged in a lawful investigation; has reason to believe that capturing the communications will be relevant to that investigation; and can ensure that the consensual monitoring will acquire only those communications that are transmitted to or from the hacker. On top of these requirements, section 217 then goes one step further. Based on the definition of a "computer trespasser," section 217 does not allow law enforcement to come to the immediate aid of victims who are being hacked by one or more of their own customers. In those cases the owner or operator of the computer system cannot provide sufficient consent to monitor the trespasser, even if the hacker/customer broke into areas of the computer he has no authority to see (including other customer account information).

Still, despite this last limitation, the hacker trespasser exception has been an important tool for law enforcement to obtain evidence based on the consent of the victim, much of which involves protecting people's privacy.

A diverse array of real-world examples from our criminal investigations demonstrate that this provision has been significant in order for the FBI to protect the privacy rights of individuals and businesses whose computers are being broken into for the purpose of stealing the personal data stored on their computers. Hackers have no respect for your privacy or mine. When hackers break into a computer network and obtain root access they get to look at, download, and even can make changes to, whatever information is on that network. Hackers can and do routinely steal social security numbers, credit card numbers, and drivers license numbers. Depending on the systems they break into, they can look at health care information and can change it at will. There has been an outpouring of concern from the American public to protect them from identity theft and to ensure that their personal records are secure. Congress has responded with a powerful array of laws that are designed to impose serious consequences on computer hackers. However, if law enforcement does not have the ability to quickly spot and then locate hackers, then the victim toll will mount and only the hackers themselves, remaining anonymous, will be left with privacy. The FBI understands the importance of preventing criminals from stealing and selling our information, and we are resolved to catch those who do. Section 217 is of enormous help in this regard.

For example, under this provision, the FBI was able to monitor the communications of an international group of "carders" (individuals that use and trade stolen credit card information).

The group used chat rooms and fraudulent websites to commit identity theft, but managed to provide themselves with privacy by using false names to get e-mail accounts. The most important tool in their bid to remain anonymous was their use of a proxy server they broke into and then reconfigured. The identity thieves used the proxy server to disguise where all of their Internet communications were coming from. The owner of the proxy server was himself a victim of the crime, his computer having essentially been hijacked and transformed into the hub of a criminal operation. When he determined that his computer had been hacked he provided the FBI with consent to monitor the intruder and hopefully to catch him. The computer owner's ability to bring in the FBI paid off, not just for him but for the countless other victims of the identity thief. By taking advantage of hacker trespasser monitoring, the FBI gathered leads that resulted in the discovery of the true identity of the subject. The subject was later indicted and is now awaiting trial.

Since its enactment, section 217 has played a key role in a variety of hacking cases, including investigations into hackers' attempts to compromise military computer systems. Allowing section 217 to expire at the end of this year would help computer hackers avoid justice and prevent law enforcement from responding quickly to victims who are themselves asking for help.

SECTION 220 -- SEARCH WARRANTS FOR ELECTRONIC EVIDENCE LOCATED IN ANOTHER DISTRICT

Lastly, I would like to turn to section 220 of the USA PATRIOT Act. Section 220 enables federal courts -- with jurisdiction over an investigation -- to issue a search warrant to compel the production of information (such as unopened e-mail) that is stored with a service provider located outside their district. The practical effect of this section is that our FBI Agents are no longer limited to applying for a search warrant solely from the court that sits where the service provider happens to be located.

Before discussing this section in depth, I think it is helpful to point out that the borderless nature of Internet crime means that more often than not *the victim* of a crime, the person who committed the crime, and *the evidence* of that crime are all located in different parts of the country (or indeed the world). Applying this fact in the context of a search warrant will demonstrate the utility and the necessity of section 220.

Prior to the PATRIOT Act, if an investigator wanted to obtain the contents of unopened e-mail from a service provider located in the United States, he or she needed to obtain a warrant from a court physically located in the same federal district as the service provider was located. To accomplish this, the FBI Agent working on the case (this Agent typically would be located where the victim is located) needed to brief another FBI Agent and prosecutor who were located in the ISP's jurisdiction (where the evidence happened to be electronically stored). The second FBI Agent and prosecutor then would appear before their local court to obtain the search warrant. This was a time and labor consuming process. Furthermore, because several of the largest email providers are located in a few districts, such as the Northern District of California and the Eastern District of Virginia, these FBI Agents, Prosecutors, and Judges were faced with a substantial workload dealing with cases in which neither the victim nor the criminal resided, and they had to be brought up to speed about the details of an investigation which, both beforehand and afterwards,

they had no need to know.

Section 220 fixed this problem. It makes clear, for example, that a judge with jurisdiction over a kidnaping investigation in Pittsburgh can issue a search warrant for e-mail messages that are stored on a server in California. As a result, the investigators in Pennsylvania can ask the judge most familiar with the investigation to issue the warrant rather than having to ask an Assistant United States Attorney in California, who is unfamiliar with the case, to ask a district judge in California, who also is unfamiliar with the case, to issue the warrant. Lest you think this is merely a hypothetical example, it's not. Using section 220, our FBI office in Pittsburgh was able to obtain a warrant for information residing on a computer in California that ultimately led to the rescue of a teenage girl who was being sexually tortured in Virginia while being chained to a wall in somebody's basement. The man who held her hostage is now in prison, serving close to 20 years. The girl's life was saved.

Other FBI Field Offices also have repeatedly stated that section 220 has been very beneficial to quickly obtain information required in their investigations. The value of this provision in terrorism cases already has been demonstrated time and again. In his April 6 testimony, Attorney General Gonzales pointed to its important application during investigations into the Portland Terror Cell, the "Virginia Jihad", and the Richard Reid "shoebomber" case.

It is imperative that section 220 be renewed. The provision expedites the investigative process and, in doing so, makes it more likely that evidence will still be available to law enforcement after it executes a court-authorized search warrant and obtains further leads; the provision frees up FBI, U.S. Attorney, and judicial personnel to more efficiently pursue other time-sensitive investigative matters; and, section 220 in no way lowers the protections that apply to the government's application for a search warrant.

CONCLUSION

Mr. Chairman and Members of the Committee, the provisions of the USA Patriot Act I have discussed today have proven significant to a number of our successes and I have every reason to believe that the need to retain these provisions in the future is also significant. By responsibly using the statutes provided by Congress, the FBI has made substantial progress in its ability to enforce the law and protect lives, while at the same time protecting civil liberties. In renewing those provisions scheduled to "sunset" at then end of this year, Congress will ensure that the FBI will continue to have the tools it needs to combat the very real threats to America and our fellow citizens. Thank you for your time today.