

Testimony of

# **The Honorable Alice Fisher**

October 9, 2002

Chairman Feinstein, Ranking Member Kyl and distinguished members of the Senate Judiciary Subcommittee on Technology, Terrorism and Government Information, I am honored to appear before you to testify about the Department of Justice's implementation and use of the important anti-terrorism provisions in the USA PATRIOT Act. I want to thank this Subcommittee's members, who helped to develop and enact the USA PATRIOT so swiftly in the wake of last September's attacks. As Deputy Assistant Attorney General of the Criminal Division, with responsibility over the Terrorism and Violent Crimes Section, I have been personally involved in seeing that the tools Congress provided in the Act have been used as intended: to enhance the ability of law enforcement to bring terrorists and other criminals to justice.

The unprecedented and heinous attacks on our nation, in which over three thousand innocent civilians were killed in New York City, in Pennsylvania, and at the Pentagon, occurred just over one year ago. At that time, the President pledged to the American people that we would not relent until justice was done and our nation was secure. Members of this Committee, and the Congress in general, joined the President as key partners in this important undertaking. Congress's swift and comprehensive response, through passage of the USA PATRIOT Act, provided us with vital new tools, and updated those tools already at our disposal, that have been instrumental to our efforts to combat terrorism in the most extensive criminal investigation in history. As the President stated when he signed the USA PATRIOT Act on October 26, 2001, we took "an essential step in defeating terrorism, while protecting the constitutional rights of Americans." One year later, I am pleased to report that we have used these tools effectively, aggressively and responsibly.

As the Attorney General told the Senate Judiciary Committee in July, the Department's single and overarching goal since September 11 has been to prevent future terrorist attacks on the United States and its citizens. We have been aggressively implementing the USA PATRIOT Act from the outset. Following its passage, we immediately sent field guidance to United States Attorney's offices, advising them of the Act's new authorities and urging their use, where appropriate, in investigating and prosecuting terrorism and other criminal acts. We have followed up with additional guidance and training over the past year, and we consult informally with federal prosecutors and investigators at work in the field investigating suspected terrorists. Our manual proved invaluable in ensuring that prosecutors around the country could immediately benefit from and utilize the new law enforcement tools provided by the Act.

Law enforcement has been engaged in an ongoing cooperative effort to identify, disrupt and dismantle terrorist networks. We are expending every effort and devoting all available resources to intercept terrorists and defend our nation. Never was this so apparent as last Friday, a defining day in the war on terrorism, when we neutralized a suspected terrorist cell in Portland, Oregon, convicted attempted suicide bomber Richard Reid, and saw John Walker Lindh, an American captured fighting for the Taliban in Afghanistan, sentenced to twenty years' imprisonment. In the last six weeks, we have charged 17 individuals involved in terrorism-related activities. In addition to Portland, we have broken up terrorist cells in Detroit and Buffalo, and we have

charged an individual with attempting to set up an Al Qaeda terrorist training camp in Oregon. Enhanced penalties authorized by the USA PATRIOT Act have proven an important tool in all of these cases.

Today, I will provide a brief summary of the Department's work to date implementing the new powers authorized by the USA PATRIOT Act. I cannot, of course, disclose information that might compromise or undermine ongoing criminal investigations and prosecutions. However, I can discuss a number of areas in which the Department of Justice, in conjunction with other departments and agencies, is making meaningful headway in the war on terrorism. In particular, over the past year, the Department has used the following important new authorities and tools provided by the Act:

- ? we have charged a number of individuals with crimes under 18 U.S.C. §§2339A and 2339B, which prohibit providing material support to terrorists or terrorist organizations, and carry enhanced penalties;

- ? we have used newly streamlined authority to use trap and trace orders to track communications of a number of criminals, including the terrorist kidnappers and murderers of journalist Daniel Pearl, as well as identity thieves and a four-time murderer;

- ? we have used new authority to subpoena information about Internet users' network addresses to track down terrorists and computer hackers;

- ? we have used newly authorized nationwide search warrants for terrorist investigations at least three times, including during the ongoing anthrax investigation;

- ? we have utilized provisions in the Act to foster an unprecedented level of cooperation and information sharing between government agencies; and

- ? we have saved precious time and resources through a provision that permits officials to obtain court orders for electronic surveillance pertaining to a particular suspect, rather than a particular device.

I will focus my testimony on four key areas in which the USA PATRIOT Act has aided law enforcement efforts: (1) it updated the law to reflect new technology; (2) it removed obstacles to investigating terrorism; (3) it strengthened criminal laws and enhanced penalties; and (4) it facilitated increased intelligence sharing, gathering and analyzing. The fifth key area, protecting our borders, falls within the bailiwick of the INS, which is also presenting testimony today.

#### 1. Updating the Law to Reflect New Technology

First, the USA PATRIOT Act allowed us to modernize our badly outmoded surveillance tools. Terrorists engaged in covert multinational operations use advanced technology, particularly in their communications and planning. While terrorists who were plotting against our nation traveled across the globe, carrying laptop computers and using disposable cell phones, federal investigators operated under laws seemingly frozen in an era of telegrams and switchboard operators. Prior to September 11, we operated both at a technological disadvantage and under legal barriers that severely restricted our surveillance capabilities. In particular, we did not have sufficiently sophisticated abilities to monitor communications in either the digital or analog world, and law enforcement officials operated under onerous rules that hindered their ability to conduct investigations in a timely manner. The USA PATRIOT Act modernized existing law, and

gave investigators crucial new tools to deal with these problems. We have put this new authority to good use.

Prior to the USA PATRIOT Act, for example, federal law required officers to spend critical time going through the burdensome process of obtaining wiretap orders to access unopened voice-mail. Now, just as had already been the case with email messages, pursuant to section 209 of the PATRIOT Act, officers can use search warrants to expedite the seizure of voice mail. Federal investigators have used these warrants in a variety of criminal cases, including both foreign and domestic terrorism cases.

Similarly, section 220 of the Act, which permits a law enforcement officer to execute a search warrant for electronic evidence outside of the district that issued the warrant, has proved crucial to dealing with the post-September 11 deluge of search warrant applications seeking evidence stored in computers, or transmitted through the Internet. Before the PATRIOT Act, because a court sitting in one district could not issue a warrant that was valid in another district, officers' access to critical information in the Internet era was unnecessarily delayed and obstructed, as the physical infrastructure, such as servers used by internet service providers, were often located thousands of miles from the scene of the crime under investigation. Even though the internet is a far-flung communications network, with access available to anyone with a properly equipped personal computer, the federal courts in those districts in which ISPs happened to locate their servers (such as in northern California) were required to handle requests for warrants in investigations all across the country. The efficiency resulting from the Act's simple modifications to existing law was invaluable in several time-sensitive investigations, including one involving a dangerous fugitive and another involving a hacker who used stolen trade secrets to extort a company.

The USA PATRIOT Act also modernized the legal requirements for pen register and trap and trace orders, streamlining this authority by clarifying that it can be used in a variety of new communications forms, not just on telephone lines, and by permitting a single order nationwide. These devices - which reveal, for example, the numbers dialed by a particular telephone or the email address to which an account sends messages - allow investigators to identify patterns of suspicious behavior or connections with known terrorists or terrorist organizations. The Department has used this improved tool to trace communications of a number of criminals, including kidnappers who communicated their demands via email, terrorist conspirators, at least one major drug distributor, identity thieves, a four-time murderer, and a fugitive who fled on the eve of trial using a fake passport. This new provision also allowed prosecutors in the Daniel Pearl case to get information critical in the identification of some of those individuals responsible for his kidnaping and murder.

The USA PATRIOT Act has updated federal law for the digital era by expediting the government's ability to execute orders requiring the help of third parties, such as telecommunications companies, in terrorism investigations. Under previous law, if an officer wanted to enlist the help of third parties to monitor a suspect, the officer had to seek specific court orders for every information source the suspect could potentially utilize. Section 206 of the Act abolished this requirement by permitting officers to simply obtain a court order pertaining to the suspect, not the particular device or devices used. This new authority allows us to avoid unnecessary cat-and-mouse games with terrorists who are trained to thwart surveillance by rapidly changing hotels or residences, cell phones, and Internet accounts before important meetings or communications.

Other provisions, such as section 211, which clarifies that the Electronic Communications

Privacy Act, not the Cable Act, governs the disclosure of information regarding communication services provided by cable companies, and section 212, which allows internet providers to disclose records to law enforcement in emergencies presenting a risk to life or limb, have made it much easier for third party communication providers to assist law enforcement without fear of civil liability. The latter authority, for example, allowed us to track down a student who posted electronic bulletin board threats to bomb his high school and shoot a faculty member and several students. Afraid of being sued, the owner and operator of the Internet message board initially resisted disclosing to federal law enforcement officials the evidence that could lead to the identification of the threat-maker. However, after he was told about the new USA PATRIOT Act emergency authority, he voluntarily disclosed to law enforcement Internet addressing information that was instrumental in the student's timely arrest and confession and in preventing the student from potentially carrying out his violent threats.

Finally, the USA PATRIOT Act has brought the federal wiretap statute into the 21st century by adding terrorism crimes to the list of offenses for which wiretap orders are available. These provisions have proven extremely useful to law enforcement officials. At least one recent wiretap order has been issued based on this expanded list of terrorism offenses. We believe that these enhancements will bring more terrorists to justice and prevent them from inflicting major damage on the infrastructure of telecommunications providers.

## 2. Removing Obstacles to Investigating Terrorism

Second, the USA PATRIOT Act has removed various obstacles to investigating terrorism and has greatly enhanced the Department's ability to thwart, disrupt, weaken, and eliminate the infrastructure of terrorist organizations. Section 219, for example, which allows federal judges to issue nationwide search warrants for physical searches in terrorism investigations, has enabled investigators to avoid expending precious time petitioning multiple judges in multiple districts for warrants. We have used this provision at least three times, including during the ongoing anthrax investigation. In that case, agents were able to obtain a search warrant from a federal judge in Washington, D.C. in order to investigate the premises of America Media, Inc. in Boca Raton, Florida. Timely action is often of the essence in law enforcement investigations and this new authority will prove invaluable.

Prior to the USA PATRIOT Act, we faced significant barriers in our ability to exclude or remove terrorists because of various statutory loopholes in the definitions concerning terrorism. Section 411 of the USA PATRIOT Act addressed these problems by expanding the grounds of inadmissibility of aliens to include those who provide assistance to terrorist organizations. At the Attorney General's request, the Department of State has listed 46 entities as terrorist organizations pursuant to authority under this provision. Members of these organizations are now denied admission to the United States for any purpose.

We believe that a number of other areas, such as greater authority to collect DNA samples from federal prisoners convicted of certain terrorism offenses under section 503, greater ability to pay rewards to help punish terrorists under sections 501 and 502, enhanced capabilities to investigate computer fraud pursuant to section 506, which permits joint Secret Service-FBI cooperation in investigations, and greater access to education information and statistics under sections 507 and 508, likewise will prove very useful in our efforts. While we have not yet had to use all of the Act's provisions, we know that they will serve as vital tools should the need arise.

## 3. Strengthening the Criminal Laws against Terrorism.

Third, the USA PATRIOT Act substantially strengthened criminal law, helping us pursue criminals in the most extensive criminal investigation in history. Critical to our efforts is the

enhanced ability to prosecute and punish terrorists captured abroad as well as those arrested within our borders. These provisions have proven to be powerful new weapons in our fight against international terrorism as well as other kinds of international criminal activity. Enhanced criminal laws relating to terrorist financing, for example, have provided an effective tool in getting law enforcement inserted into the early stages of terrorist planning. Title III of the USA PATRIOT Act provides law enforcement with important new authority to investigate and prosecute the financing of terrorism. We can now seize terrorist assets, both foreign and domestic, if the property or its owner is involved in, related to, or in support of acts of domestic or international terrorism. It is now a crime for anyone subject to U.S. jurisdiction to provide anything of value - including their own efforts or expertise - to organizations designated as "foreign terrorist organization." This is true regardless of whether the persons providing such support intend their donations to be used for violent purposes, or whether actual terrorism results. If someone subject to U.S. jurisdiction provides, or even attempts to provide, any material support or resources to Hamas, Hizballah, Al Qaeda, the Abu Sayyaf Group or any of the other designated groups, that person can be prosecuted. And our prosecutors do not have to prove that the support actually went to specific terrorist acts. The Department has used this provision in prosecuting a number of Al Qaeda associated individuals and in breaking up terrorist cells in this country. For example, John Walker Lindh, the American citizen who joined the Taliban and was captured by military forces in Afghanistan, was charged with 10 counts, including a total of six relating to providing material support to individuals and to organizations that commit crimes of terrorism. Lindh, who pled guilty to providing services to the Taliban and to carrying an explosive while engaged in the commission of a felony, was sentenced last Friday to 20 years imprisonment. On August 28, 2002, we charged Ernest James Ujaama with providing material support to Al Qaeda by, among other things, attempting to set up an Al Qaeda terrorist training camp at a farm in Oregon. On that same day, five Detroit men affiliated with Al Qaeda were charged with providing material support or resources to terrorists. On September 13, 2002, six United States citizens in the Buffalo area, who are believed to be part of another Al Qaeda-affiliated cell, were arrested on charges of providing support or resources to terrorists. And just last Friday, we indicted six individuals in Portland, Oregon, also affiliated with Al Qaeda, with providing material support or resources to terrorists.

Our ability to fight transnational crime was further enhanced by making the smuggling of bulk cash across our border unlawful, adding terrorism and other offenses to the list of racketeering offenses, and providing prosecutors with the authority to seize money subject to forfeiture in a foreign bank account by authorizing the seizure of such a foreign bank's funds held in a U.S. correspondent account. Another important provision expanded our ability to prosecute unlicensed money transmitters by enhancing section 1960 of Title 18. We used this revised statute successfully in the District of Massachusetts. On November 18, 2001, a federal grand jury returned an indictment charging Liban Hussein, the local president of an Al Barakaat money remitting house, and his brother, Mohamed Hussein, with a violation of § 1960. This prosecution was part of a national, and indeed international, enforcement action against the Al Barakaat network, which has financed the operations of Al Qaeda and other terrorist organizations. Mohamed Hussein was convicted and sentenced to 18 months' incarceration for operating an unlicensed money remitting business. His brother is a fugitive.

Title III of the Act also permits the forfeiture of funds held in United States interbank accounts. We used this provision to prosecute James Gibson, who had defrauded clients of millions of dollars by fraudulently structuring settlement for numerous personal injury victims. After he and

his wife fled to Belize and deposited some of the monies from the scheme in two Belizean banks, we were able to have a seizure warrant served on the bank's interbank account in the United States and recover remaining funds.

We have attempted to use section 801, which makes it a federal offense to engage in terrorist attacks and other acts of violence against mass transportation systems, in at least one high profile case. One of the counts brought against "shoe bomber" Richard Reid, who was charged for concealing a bomb in his shoe during a transatlantic flight, alleged a violation of terrorist attacks and other acts of violence against mass transportation systems. This charge was dismissed after the judge determined that the definition of mass transportation does not include airplanes. In the meantime, Richard Reid pleaded guilty to the remaining counts brought against him last Friday. He will be sentenced in January and faces a sentence of 60 years to life.

We will continue to use these enhanced capabilities to bring those associated with terrorism to justice.

4. Enhancing the Capacity of Law Enforcement to Gather, Analyze and Share Intelligence Finally, and perhaps most significantly, the USA PATRIOT Act allowed us to significantly enhance our capability to share information and coordinate our efforts. Immediately following the September 11 attacks, the Attorney General ordered a top-to-bottom review and reorganization of the Department of Justice in order to effectively mobilize our law enforcement resources and justice system. The Attorney General's review found that restrictions imposed decades ago were severely impeding our intelligence gathering and sharing capabilities. As FBI Director Mueller stated several weeks ago before the House Financial Services Committee, "creating an alliance between law enforcement and intelligence agencies is the key to dismantling terrorist organizations and eliminating the threat they pose."

The USA PATRIOT Act fosters this communication across agency lines, breaking down once formidable barriers previously in place. Prior to last October, there was no mechanism for sharing certain types of criminal investigative material with the intelligence community, and the intelligence community could not easily open their files to law enforcement. Sharing was possible, but only in limited situations and through onerous procedures that diverted resources from investigative activity. The loosening of these procedures under section 203 of the USA PATRIOT Act has been invaluable. We are now enjoying an unprecedented level of cooperation and information-sharing between and among U.S. government agencies involved in counter-terrorism. The Department, for example, has made disclosures of information obtained through grand juries and involving foreign intelligence on over forty occasions, and in compliance with section 203, we have filed disclosure notices or obtained prior approval from the courts in at least 38 districts.

On September 23, 2002, the Attorney General announced three new guidelines designed to institutionalize the ongoing sharing of information between federal law enforcement and the U.S. intelligence community. These guidelines formalize the existing framework for information sharing to ensure that vital intelligence information ends up in the hands of those officials who need it most, while respecting the interests generally protected by grand jury secrecy and wiretap rules.

The Act also allocated funds to the FBI to help facilitate information sharing with the INS and State Department via the National Crime Information Center (NCIC). Access to these files has enabled agencies to better determine whether a visa applicant has a criminal history record. The importance of this system cannot be underestimated. It is the nation's principal law enforcement automated information sharing tool. On April 11, 2002, the Attorney General issued a major

directive on the coordination of information relating to terrorism that requires all investigative components within the Department of Justice to provide the names, photographs, and other identifying data of all known or suspected terrorists for inclusion in the database. Since enactment, the FBI has provided the State Department with over 8.4 million records from these databases, and has provided 83,000 comprehensive records of key wanted persons in the databases, as well as information regarding military detainees in Afghanistan, Pakistan, and Guantanamo Bay to the INS.

The USA PATRIOT Act has also improved the effectiveness of the Foreign Intelligence Surveillance Act by permitting the authorization of physical searches and electronic surveillance of foreign powers' employees for up to 120 days, as opposed to the previous 45 days. This additional leeway gives government investigators targeting potential terrorist activity additional time and helps clear court dockets for more far-reaching terrorism related cases and other complex federal prosecution. While the details of FISA operations are classified, I can tell you that this improvement has saved critical time that law enforcement previously spent continuously renewing court orders. Additionally, section 218, which broadened the applicable standard under which law enforcement could conduct FISA surveillance or searches, has reduced officers' need to weigh constantly the purposes of their investigation, and has allowed for increased collaboration between law enforcement and intelligence personnel.

#### Conclusion

I would like to conclude by thanking the members of this Committee for your efforts in so swiftly developing and passing the USA PATRIOT Act in the wake of last year's attacks on our nation. Your response enabled those of us whose mission it is to combat terrorists at home and abroad to do so with a wide array of new measures that have greatly enhanced our ability to carry out this work. We look forward to continuing to work with the Committee in this collaborative effort. I thank you for your invitation and welcome any questions that you may have.