Department of Justice

STATEMENT

OF

JAMES A. BAKER
COUNSEL FOR INTELLIGENCE POLICY
OFFICE OF INTELLIGENCE POLICY AND REVIEW
UNITED STATES DEPARTMENT OF JUSTICE

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY
COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

CONCERNING

THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, PART II:
(USA PATRIOT ACT §§ 206 AND 215)

PRESENTED ON

APRIL 28, 2005

Testimony of
James A. Baker
Counsel for Intelligence Policy
Office of Intelligence Policy and Review
United States Department of Justice
before the
Subcommittee on Crime, Terrorism, and Homeland Security
Committee on the Judiciary
United States House of Representatives

April 28, 2005

Chairman Coble, Ranking Member Scott, and Members of the Committee:

I am pleased to be here today to discuss the government's use of authorities granted to it by Congress under the Foreign Intelligence Surveillance Act of 1978 (FISA). In particular, I appreciate the opportunity to have a candid discussion about the impact of the amendments to FISA under the USA PATRIOT Act and how critical they are to the government's ability to successfully prosecute the war on terrorism and prevent another attack like that of September 11 from happening again.

As Counsel for Intelligence Policy in the Department of Justice, I am head of the Office of Intelligence Policy and Review (OIPR). OIPR conducts oversight of the intelligence and counterintelligence activities of the Executive Branch agencies including the FBI. We prepare all applications for electronic surveillance and physical search under FISA and represent the government before the Foreign Intelligence Surveillance Court (FISA Court). OIPR reports directly to the Deputy Attorney General. I am a career member of the Senior Executive Service, not a political appointee.

I. FISA Statistics

As I noted in my testimony before this Subcommittee on Tuesday, since September 11, the volume of applications to the FISA Court has dramatically increased from 1,012 applications for surveillance or search filed under FISA in 2000 to 1,758 applications in 2004.

II. Key Uses of FISA Authorities in the War on Terrorism

In enacting the USA PATRIOT Act, the Intelligence Authorization Act for Fiscal Year 2002, and the Intelligence Reform and Terrorism Prevention Act of 2004, Congress provided the government with vital tools that it has used regularly and effectively in its war on terrorism. The reforms in those measures affect every single application made by the Department for electronic surveillance or physical search of suspected terrorists and have enabled the government to become quicker and more flexible in gathering critical intelligence information on suspected terrorists. It is because of the key importance of these tools to winning the war on terror that the

Department asks you to reauthorize the USA PATRIOT Act provisions scheduled to expire at the end of this year. Today, it is my understanding the Committee wishes to discuss sections 206 and 215 of the USA Patriot Act. Both provisions are scheduled to sunset at the end of the year.

A. **Roving Wiretaps** (U)

Section 206 of the USA PATRIOT Act extends to FISA the ability to "follow the target" for purposes of surveillance rather than tie the surveillance to a particular facility and provider when the target's actions may have the effect of thwarting that surveillance. As you know, in his testimony earlier this month before the Senate Judiciary Committee, the Attorney General declassified the fact that the FISA Court issued 49 orders authorizing the use of roving surveillance authority under section 206 as of March 30, 2005. Use of roving surveillance has been available to law enforcement for many years and has been upheld by several federal courts, including the Second, Fifth, and Ninth Circuits. Some object that this provision gives the FBI discretion to conduct surveillance of persons who are not approved targets of court-authorized surveillance. This is wrong. Section 206 did not alter the requirement that before approving electronic surveillance, the FISA Court must find that there is probable cause to believe that the target of the surveillance is either a foreign power or an agent of a foreign power, such as a terrorist or spy. Without this authority, investigators will once again have to struggle to catch up to sophisticated terrorists trained to constantly change phones in order to avoid surveillance.

Critics of section 206 also contend that it allows intelligence investigators to conduct "John Doe" roving surveillance that permits the FBI to wiretap every single phone line, mobile communications device, or Internet connection the suspect may use without having to identify the suspect by name. As a result, they fear that the FBI may violate the communications privacy of innocent Americans. Let me respond to this criticism in the following way. First, even when the government is unsure of the name of a target of such a wiretap, FISA requires the government to provide "the identity, if known, or a description of the target of the electronic surveillance" to the FISA Court prior to obtaining the surveillance order. 50 U.S.C. §§ 1804(a)(3) and 1805(c)(1)(A). As a result, each roving wiretap order is tied to a particular target whom the FISA Court must find probable cause to believe is a foreign power or an agent of a foreign power. In addition, the FISA Court must find "that the actions of *the target* of the application may have the effect of thwarting" the surveillance, thereby requiring an analysis of the activities of a foreign power or an agent of a foreign power that can be identified or described. 50 U.S.C. § 1805(c)(2)(B). Finally, it is important to remember that FISA has always required that the government conduct every surveillance pursuant to appropriate minimization procedures that limit the government's acquisition, retention, and dissemination of irrelevant communications of innocent Americans. Both the Attorney General and the FISA Court must approve those minimization procedures. Taken together, we believe that these provisions adequately protect against unwarranted governmental intrusions into the privacy of Americans. Section 206 sunsets at the end of this year.

B. **Access to Tangible Things**

Section 215 of the USA PATRIOT Act allows the FBI to obtain business records or other tangible things under FISA pursuant to a FISA Court order if the items relate to an ongoing authorized national security investigation, which, in the case of a United States person, cannot be based solely upon activities protected by the first amendment to the Constitution. The Attorney General also recently declassified the fact that the FISA Court has issued 35 orders under section 215 from the effective date of the Act through March 30th of this year. The Attorney General also declassified the types of business records sought by these orders. They include driver's license records, public accommodation records, apartment leasing records, credit card records, and subscriber information, such as names and addresses, for telephone numbers captured through court-authorized pen register devices. None of those orders were issued to libraries and/or booksellers, or were for medical or gun records.

Section 215 provides a tool under FISA that is similar to a grand jury subpoena in the criminal context. A prosecutor in a criminal case can issue a grand jury subpoena to obtain items relevant to his investigation. Section 215 provides a mechanism for obtaining records or items relevant to an investigation to protect against international terrorism or clandestine intelligence activities. Section 215 orders, however, are subject to greater judicial oversight than are grand jury subpoenas before they are issued. The FISA Court must explicitly authorize the use of section 215 to obtain business records before the government may serve the request on a recipient. In contrast, grand jury subpoenas are not subject to judicial review before they are issued. Section 215 orders are also subject to the same burden of proof standard as are grand jury subpoenas — a relevance standard.

Section 215, which makes no reference to libraries and booksellers, has been criticized because it does not exempt libraries and booksellers. The absence of such an exemption is consistent with criminal investigative practice. Prosecutors have always been able to obtain records from libraries and bookstores through grand jury subpoenas. Libraries and booksellers should not become safe havens for terrorists and spies. While section 215 has never been used to obtain such records, last year, a member of a terrorist group closely affiliated with al Qaeda used Internet service provided by a public library to communicate with his confederates. Furthermore, we know that spies have used public library computers to do research to further their espionage and to communicate with their co-conspirators. For example, Brian Regan, a former TRW employee working at the National Reconnaissance Office, who recently was convicted of espionage, extensively used computers at five public libraries in Northern Virginia and Maryland to access addresses for the embassies of certain foreign governments. A terrorist using a computer in a library should not be afforded greater privacy protection than a terrorist using a computer in his home.

Concerns that section 215 allows the government to target Americans because of the books they read or websites they visit are misplaced. The provision explicitly prohibits the government from obtaining a section 215 order if an investigation were to be based solely upon protected First Amendment activity. 50 U.S.C. §§ 1861(a)(2)(B). However, some criticisms of section 215 have apparently been based on possible ambiguity in the law. The Department has already stated in litigation that the recipient of a section 215 order may consult with his attorney

and may challenge that order in court. The Department has also stated that the government may seek, and a court may require, only the production of records that are relevant to a national security investigation, a standard similar to the relevance standard that applies to grand jury subpoenas in criminal cases. The text of section 215, however, is not as clear as it could be in these respects. The Department, therefore, is willing to support amendments to Section 215 to clarify these points. Section 215 is scheduled to sunset at the end of 2005.

CONCLUSION

It is critical that the elements of the USA PATRIOT Act subject to sunset in a matter of months be renewed. The USA PATRIOT has greatly enhance the government's ability to effectively wage the war on terrorism.

I thank the Committee for the opportunity to discuss the importance of the USA PATRIOT Act to this nation's ongoing war against terrorism. I appreciate the Committee's close attention to this important issue. I would be pleased to answer any questions you may have. Thank you.