



Department of Justice

STATEMENT

OF

MARY BETH BUCHANAN
UNITED STATES ATTORNEY
WESTERN DISTRICT OF PENNSYLVANIA

BEFORE THE

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

CONCERNING

THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, PART I:
(USA PATRIOT ACT §§ 204, 207, 214, 225 & THE "LONE WOLF" PROVISION)

PRESENTED ON

APRIL 26, 2005

MARY BETH BUCHANAN
UNITED STATES ATTORNEY
WESTERN DISTRICT OF PENNSYLVANIA
PREPARED REMARKS FOR THE
SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY
COMMITTEE ON THE JUDICIARY
UNITED STATES HOUSE OF REPRESENTATIVES

APRIL 26, 2005

INTRODUCTION

Mr. Chairman, Ranking Member Scott, Members of the Subcommittee, thank you for asking me here today. I am Mary Beth Buchanan, the United States Attorney in the Western District of Pennsylvania and the Director of the Executive Office for United States Attorneys. It is an honor to appear before you today to discuss how the Department has used the important provisions of the USA PATRIOT Act to better combat terrorism and other serious criminal conduct. I will specifically focus today on two of the provisions that are the subject of today's hearing – Section 214 and Section 225 of the USA PATRIOT Act – since those are two provisions that harmonized tools used in terrorism investigations with tools that have been used routinely and effectively in criminal prosecutions long before the passage of the USA PATRIOT Act.

Section 214 of the USA PATRIOT Act allows the government to obtain a pen register order in national security investigations where the information likely is relevant to an international

terrorism or espionage investigation. This provision is similar to the 1986 criminal pen register statute (18 U.S.C. § 3121) that has been frequently used by criminal prosecutors to obtain pen registers and trap and trace devices in a variety of criminal investigations. A pen register is a device that can track dialing, routing, addressing, and signaling information about a communication – for example, which numbers are dialed from a particular telephone. Pen registers are not used to collect the content of communications. Similarly, a trap-and-trace device tracks numbers used to call a particular telephone, without monitoring the substance or content of the telephone conversation. Both devices are routinely used in criminal investigations where, in order to obtain the necessary order authorizing use of the device, the government must show simply that the information sought is relevant to an ongoing investigation.

Pen registers and trap and trace devices have long been used as standard preliminary investigative tools in a variety of criminal investigations and prosecutions. In many instances, these tools are used as one of the first steps in a criminal investigation with the information gathered used to determine if more intrusive forms of surveillance, such as search warrants or wiretaps, are justified. Use of these tools may oftentimes lead investigators and prosecutors to additional suspects or targets in an investigation because of their important ability to allow prosecutors to link defendants or “connect the dots” in a conspiracy or other type of criminal offense.

To obtain a pen register or trap and trace device under 18 U.S.C. § 3121 *et seq.*, a criminal prosecutor must certify that the information sought is relevant to an ongoing criminal investigation, and upon that certification, the court enters an *ex parte* order authorizing the installation and use of a pen register or a trap and trace device. There is no requirement that the

court make a probable cause finding. Under long-settled Supreme Court precedent, the use of pen registers does not constitute a "search" within the meaning of the Fourth Amendment. As such, the Constitution does not require that the government obtain court approval before installing a pen register. The absence of a probable cause requirement is justified because the devices merely obtain information that is voluntarily disclosed to the telephone service provider. Therefore, there is no reasonable expectation of privacy in the information.

Currently under FISA, government officials similarly may seek a court order for a pen register or trap-and-trace device to gather foreign intelligence information or information about international terrorism or espionage. Prior to enactment of the USA PATRIOT Act, however, FISA required government personnel to certify not just that the information they sought was relevant to an intelligence investigation, but also that the facilities to be monitored had been used or were about to be used to contact a foreign agent or an agent of a foreign power, such as a terrorist or spy. Thus, it was much more difficult to obtain an effective pen register or trap-and-trace order in an international terrorism investigation than in a criminal investigation.

Section 214 of the USA PATRIOT Act brought authorities for terrorism and other foreign intelligence investigations more into line with similar criminal authorities by permitting court approval of FISA pen registers and trap-and-trace orders even though an applicant might be unable to certify at that stage of an investigation that the facilities themselves, such as phones, are used by foreign agents or those engaged in international terrorist or clandestine intelligence activities. Significantly, however, applicants must still certify that the devices are likely to obtain foreign intelligence information not concerning a U.S. person, or information relevant to an international terrorism investigation. Section 214 streamlined the process for obtaining pen

registers under FISA while preserving the existing court-order requirement that is evaluated by the same relevance standard as in the criminal context. Now as before, investigators cannot install a pen register unless they apply for and receive permission from the FISA Court. In addition, Section 214 explicitly safeguards First Amendment rights. It requires that any investigation of a United States person not be conducted solely upon the basis of activities protected by the First Amendment to the Constitution. As a result, the Department of Justice must satisfy the FISA Court that its investigation is not solely based upon First Amendment protected activity, which requires the Department to inform the Court of the justification for the investigation.

If Section 214 were allowed to expire, it would be more difficult to obtain a pen register order in an international terrorism investigation than in a criminal investigation, and investigators would have a harder time developing leads in important terrorism investigations.

Section 225 of the USA PATRIOT Act also harmonized the FISA context and criminal prosecutions--in this case extending an important provision used for years in criminal prosecutions to the FISA context. The United States may obtain electronic surveillance and physical search orders from the FISA Court concerning an entity or individual whom the court finds probable cause to believe is an agent of a foreign power. Generally, however, as in the case of criminal wiretaps and electronic surveillance, the United States requires the assistance of private communications providers to carry out such court orders. In the criminal and civil contexts, those who disclose information pursuant to a subpoena or court order are generally exempted from liability. For example, those assisting the government in carrying out criminal investigative wiretaps are provided with immunity from civil liability. This immunity is important because it

helps to secure the prompt cooperation of private parties with law enforcement officers to ensure the effective implementation of court orders.

Prior to the passage of the USA PATRIOT Act, however, while those assisting in the implementation of criminal wiretaps were provided with immunity, no similar immunity protected those companies and individuals assisting the government in carrying out surveillance orders issued by the FISA Court under FISA. Section 225 ended this anomaly by providing immunity to those who assist the government in implementing FISA surveillance orders, thus ensuring that such entities and individuals will comply with orders issued by the FISA Court without delay. This immunity is important because it helps to secure the prompt cooperation of private parties, such as telephone companies, whose assistance is necessary for the effective implementation of court orders. For example, in the investigation of an espionage subject, the FBI was able to convince a company to assist in the installation of technical equipment pursuant to a FISA order by providing a letter outlining the immunity from civil liability associated with complying with the FISA order. Section 225 has been praised for protecting those companies and individuals who are simply fulfilling their legal obligations. If section 225 is allowed to expire, it would be more difficult for the Department of Justice to implement FISA surveillance orders in a timely and effective manner. Because Section 225 simply extends to the FISA context the exemption long applied in the civil and criminal contexts, where individuals who disclose information pursuant to a subpoena or court order generally are immune from liability for disclosure, it should be made permanent.

I thank you for inviting me here and giving me the opportunity to explain in concrete terms how the USA PATRIOT Act has changed the way we fight terrorism. I hope you agree that there is no good reason for investigators to have fewer tools to use in terrorism investigations than they have long used in criminal investigations. Fortunately, the USA PATRIOT Act was passed by Congress to correct these flaws in the system. Now that we have fixed this process, we can't go back. We must continue to pursue the terrorists with every legal means available. The law enforcement community needs the important tools of the USA PATRIOT Act to continue to keep our nation safe from attack.

I thank this Committee for its continued leadership and support. I will be happy to respond to any questions you may have.

Testimony of Alberto R. Gonzales, Attorney General of the United States
and Robert S. Mueller, III, Director, Federal Bureau of Investigation
United States Department of Justice
Before the Select Committee on Intelligence
United States Senate
April 27, 2005

Chairman Roberts, Vice Chairman Rockefeller, and Members of the Committee:

We are 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, we appreciate the opportunity to have a candid discussion about the impact of the amendments to FISA made by 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 ever happening again.

As we stated in our testimony to the Senate Judiciary Committee, we are open to suggestions for strengthening and clarifying the USA PATRIOT Act, and we look forward to meeting with people both inside and outside of Congress who have expressed views about the Act. However, we will not support any proposal that would undermine our ability to combat terrorism effectively.

I. FISA Statistics

First, we would like to talk with you about the use of FISA generally. Since September 11, the volume of applications to the Foreign Intelligence Surveillance Court (FISA court) has dramatically increased.

- In 2000, 1,012 applications for surveillance or search were filed under FISA. As the Department's public annual FISA report sent to Congress on April 1, 2005 states, in 2004 we filed 1,758 applications, a 74% increase in four years.
- Of the 1,758 applications made in 2004, none were denied, although 94 were modified by the FISA court in some substantive way.

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 contained 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 the war on terror that we ask you to reauthorize the provisions of the USA PATRIOT Act scheduled to expire at the

end of this year. Of particular concern is section 206's authorization of multipoint or "roving" wiretaps, section 207's expansion of FISA's authorization periods for certain cases, section 214's revision of the legal standard for installing and using pen register / trap and trace devices, and section 215's grant of the ability to obtain a Court order requesting the production of business records related to national security investigations.

In addition, the Intelligence Reform and Terrorism Prevention Act of 2004 includes a "lone wolf" provision that expands the definition of "agent of a foreign power" to include a non-United States person, who acts alone or is believed to be acting alone and who engages in international terrorism or in activities in preparation therefor. This provision is also scheduled to sunset at the end of this year, and we ask that it be made permanent as well.

A. Roving Wiretaps

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. In the Attorney General's testimony at the beginning of this month before the Senate Judiciary Committee, he 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 as constitutional 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 change 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 section 206, 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. Authorized Periods for FISA Collection

Section 207 of the USA PATRIOT Act has been essential to protecting the national security of the United States and protecting the civil liberties of Americans. It changed the time periods for which electronic surveillance and physical searches are authorized under FISA and, in doing so, conserved limited OIPR and FBI resources. Instead of devoting time to the mechanics of repeatedly renewing FISA applications in certain cases -- which are considerable -- those resources can be devoted instead to other investigative activity as well as conducting appropriate oversight of the use of intelligence collection authorities by the FBI and other intelligence agencies. A few examples of how section 207 has helped are set forth below.

Since its inception, FISA has permitted electronic surveillance of an individual who is an agent of foreign power based upon his status as a non-United States person who acts in the United States as "an officer or employee of a foreign power, or as a member" of an international terrorist group. As originally enacted, FISA permitted electronic surveillance of such targets for initial periods of 90 days, with extensions for additional periods of up to 90 days based upon subsequent applications by the government. In addition, FISA originally allowed the government to conduct physical searches of any agent of a foreign power (including United States persons) for initial periods of 45 days, with extensions for additional 45-day periods.

Section 207 of the USA PATRIOT Act changed the law as to permit the government to conduct electronic surveillance and physical search of certain agents of foreign powers and non-resident alien members of international groups for initial periods of 120 days, with extensions for periods of up to one year. It also allows the government to obtain authorization to conduct a physical search of any agent of a foreign power for periods of up to 90 days. Section 207 did not change the time periods applicable for electronic surveillance of United States persons, which remain at 90 days. By making these time periods equivalent, it has enabled the Department to file streamlined combined electronic surveillance and physical search applications that, in the past, were tried but abandoned as too cumbersome to do effectively.

As the Attorney General testified before the Senate Judiciary Committee, we estimate that the amendments in section 207 have saved OIPR approximately 60,000 hours of attorney time in the processing of applications. Because of section 207's success, we have proposed additional amendments to increase the efficiency of the FISA process. Among these would be to allow coverage of all non-U.S. person agents for foreign powers for 120 days initially with each

renewal of such authority allowing continued coverage for one year. Had this and other proposals been included in the USA PATRIOT Act, the Department estimates that an additional 25,000 attorney hours would have been saved in the interim. Most of these ideas were specifically endorsed in the recent report of the WMD Commission. The WMD Commission agreed that these changes would allow the Department to focus its attention where it is most needed and to ensure adequate attention is given to cases implicating the civil liberties of Americans. Section 207 is scheduled to sunset at the end of this year.

C. Pen Registers and Trap and Trace Devices

Some of the most useful, and least intrusive, investigative tools available to both intelligence and law enforcement investigators are pen registers and trap and trace devices. These devices record data regarding incoming and outgoing communications, such as all of the telephone numbers that call, or are called by, certain phone numbers associated with a suspected terrorist or spy. These devices, however, do not record the substantive content of the communications, such as the words spoken in a telephone conversation. For that reason, the Supreme Court has held that there is no Fourth Amendment protected privacy interest in information acquired from telephone calls by a pen register. Nevertheless, information obtained by pen registers or trap and trace devices can be extremely useful in an investigation by revealing the nature and extent of the contacts between a subject and his confederates. The data provides important leads for investigators, and may assist them in building the facts necessary to obtain probable cause to support a full content wiretap.

Under chapter 206 of title 18, which has been in place since 1986, if an FBI agent and prosecutor in a criminal investigation of a bank robber or an organized crime figure want to install and use pen registers or trap and trace devices, the prosecutor must file an application to do so with a federal court. The application they must file, however, is exceedingly simple: it need only specify the identity of the applicant and the law enforcement agency conducting the investigation, as well as "a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency." Such applications, of course, include other information about the facility that will be targeted and details about the implementation of the collection, as well as "a statement of the offense to which the information likely to be obtained . . . relates," but chapter 206 does not require an extended recitation of the facts of the case.

In contrast, prior to the USA PATRIOT Act, in order for an FBI agent conducting an intelligence investigation to obtain FISA authority to use the same pen register and trap and trace device to investigate a spy or a terrorist, the government was required to file a complicated application under title IV of FISA. Not only was the government's application required to include "a certification by the applicant that the information likely to be obtained is relevant to an ongoing foreign intelligence or international terrorism investigation being conducted by the Federal Bureau of Investigation under guidelines approved by the Attorney General," it also had to include the following:

information which demonstrates that there is reason to believe that the telephone line to which the pen register or trap and trace device is to be attached, or the communication instrument or device to be covered by the pen register or trap and trace device, has been or is about to be used in communication with—

(A) an individual who is engaging or has engaged in international terrorism or clandestine intelligence activities that involve or may involve a violation of the criminal laws of the United States; or

(B) a foreign power or agent of foreign power under circumstances giving reason to believe that the communication concerns or concerned international terrorism or clandestine intelligence activities that involve or may involve a violation of the criminal laws of the United States.

Thus, the government had to make a much different showing in order obtain a pen register or trap and trace authorization to find out information about a spy or a terrorist than is required to obtain the very same information about a drug dealer or other ordinary criminal. Sensibly, section 214 of the USA PATRIOT Act simplified the standard that the government must meet in order to obtain pen/trap data in national security cases. Now, in order to obtain a national security pen/trap order, the applicant must certify “that the information likely to be obtained is foreign intelligence information not concerning a United States person, or is relevant to an investigation to protect against international terrorism or clandestine intelligence activities.” Importantly, the law requires that such an investigation of a United States person may not be conducted solely upon the basis of activities protected by the First Amendment to the Constitution.

Section 214 should not be permitted to expire and return us to the days when it was more difficult to obtain pen/trap authority in important national security cases than in normal criminal cases. This is especially true when the law already includes provisions that adequately protect the civil liberties of Americans. I urge you to re-authorize section 214.

D. Access to Tangible Things

Section 215 of the USA PATRIOT Act allows the FBI to obtain an order from the FISA Court requesting production of any tangible thing, such as business records, if the items are relevant 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 declassified earlier this month the fact that the FISA Court has issued 35 orders requiring the production of tangible things under section 215 from the date of the effective date of the Act through March 30th of this year. None of those orders was issued to libraries and/or booksellers, and none was for medical or gun records. The provision to date has been used only to order the production of 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.

Similar to a prosecutor in a criminal case issuing a grand jury subpoena for an item relevant to his investigation, so too may the FISA Court issue an order requiring the production of records or items that are relevant to an investigation to protect against international terrorism or clandestine intelligence activities. Section 215 orders, however, are subject to judicial oversight before they are issued – unlike grand jury subpoenas. The FISA Court must explicitly authorize the use of section 215 to obtain business records before the government may serve the order on a recipient. In contrast, grand jury subpoenas are subject to judicial review only if they are challenged by the recipient. Section 215 orders are also subject to the same standard as grand jury subpoenas – a relevance standard.

Section 215 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. 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 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.

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 conducting an investigation of a U.S. person 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 also is scheduled to sunset at the end of this year.

E. The “Wall”

Before the USA PATRIOT Act, applications for orders authorizing electronic surveillance or physical searches under FISA had to include a certification from a high-ranking Executive Branch official that “*the purpose*” of the surveillance or search was to gather foreign

intelligence information. As interpreted by the courts and the Justice Department, this requirement meant that the “primary purpose” of the collection had to be to obtain foreign intelligence information rather than evidence of a crime. Over the years, the prevailing interpretation and implementation of the “primary purpose” standard had the effect of sharply limiting coordination and information sharing between intelligence and law enforcement personnel. Because the courts evaluated the government’s purpose for using FISA at least in part by examining the nature and extent of such coordination, the more coordination that occurred, the more likely courts would find that law enforcement, rather than foreign intelligence collection, had become the primary purpose of the surveillance or search.

During the 1980s, the Department operated under a set of largely unwritten rules that limited to some degree information sharing between intelligence and law enforcement officials. In 1995, however, the Department established formal procedures that more clearly separated law enforcement and intelligence investigations and limited the sharing of information between intelligence and law enforcement personnel even more than the law required. The promulgation of these procedures was motivated in part by the concern that the use of FISA authorities would not be allowed to continue in particular investigations if criminal prosecution began to overcome intelligence gathering as an investigation’s primary purpose. The procedures were intended to permit a degree of interaction and information sharing between prosecutors and intelligence officers while at the same time ensuring that the FBI would be able to obtain or continue FISA coverage and later use the fruits of that coverage in a criminal prosecution. Over time, however, coordination and information sharing between intelligence and law enforcement personnel became more limited in practice than was allowed in reality. A perception arose that improper information sharing could end a career, and a culture developed within the Department sharply limiting the exchange of information between intelligence and law enforcement officials.

Sections 218 and 504 of the USA PATRIOT Act helped to bring down this “wall” separating intelligence and law enforcement officials. They erased the perceived statutory impediment to more robust information sharing between intelligence and law enforcement personnel. They also provided the necessary impetus for the removal of the formal administrative restrictions as well as the informal cultural restrictions on information sharing.

Section 218 of the USA PATRIOT Act eliminated the “primary purpose” requirement. Under section 218, the government may conduct FISA surveillance or searches if foreign intelligence gathering is a “significant” purpose of the surveillance or search. This eliminated the need for courts to compare the relative weight of the “foreign intelligence” and “law enforcement” purposes of the surveillance or search, and allows increased coordination and sharing of information between intelligence and law enforcement personnel. Section 218 was upheld as constitutional in 2002 by the FISA court of Review. This change, significantly, did not affect the government’s obligation to demonstrate that there is probable cause to believe that the target is a foreign power or an agent of a foreign power. Section 504 – which is not subject to sunset – buttressed section 218 by specifically amending FISA to allow intelligence officials conducting FISA surveillances or searches to “consult” with federal law enforcement officials to

“coordinate” efforts to investigate or protect against international terrorism, espionage, and other foreign threats to national security, and to clarify that such coordination “shall not” preclude the certification of a “significant” foreign intelligence purpose or the issuance of an authorization order by the FISA court.

The Department moved aggressively to implement sections 218 and 504. Following passage of the Act, the Attorney General adopted new procedures designed to increase information sharing between intelligence and law enforcement officials, which were affirmed by the FISA court of Review on November 18, 2002. The Attorney General has also issued other directives to further enhance information sharing and coordination between intelligence and law enforcement officials. In practical terms, a prosecutor may now consult freely with the FBI about what, if any, investigative tools should be used to best prevent terrorist attacks and protect the national security. Unlike section 504, section 218 is scheduled to sunset at the end of this year.

The increased information sharing facilitated by the USA PATRIOT Act has led to tangible results in the war against terrorism: plots have been disrupted; terrorists have been apprehended; and convictions have been obtained in terrorism cases. Information sharing between intelligence and law enforcement personnel, for example, was critical in successfully dismantling a terror cell in Portland, Oregon, popularly known as the “Portland Seven,” as well as a terror cell in Lackawanna, New York. Such information sharing has also been used in the prosecution of: several persons involved in al Qaeda drugs-for-weapons plot in San Diego, two of whom have pleaded guilty; nine associates in Northern Virginia of a violent extremist group known as Lashkar-e-Taiba that has ties to al Qaeda, who were convicted and sentenced to prison terms ranging from four years to life imprisonment; two Yemeni citizens, Mohammed Ali Hasan Al-Moayad and Mohshen Yahya Zayed, who were charged and convicted for conspiring to provide material support to al Qaeda and HAMAS; Khaled Abdel Latif Dumeisi, who was convicted by a jury in January 2004 of illegally acting as an agent of the former government of Iraq as well as two counts of perjury; and Enaam Arnaout, the Executive Director of the Illinois-based Benevolence International Foundation, who had a long-standing relationship with Osama Bin Laden and pleaded guilty to a racketeering charge, admitting that he diverted thousands of dollars from his charity organization to support Islamic militant groups in Bosnia and Chechnya. Information sharing between intelligence and law enforcement personnel has also been extremely valuable in a number of other ongoing or otherwise sensitive investigations that we are not at liberty to discuss today.

While the “wall” primarily hindered the flow of information from intelligence investigators to law enforcement investigators, another set of barriers, before the passage of the USA PATRIOT Act, often hampered law enforcement officials from sharing information with intelligence personnel and others in the government responsible for protecting the national security. Federal law, for example, was interpreted generally to prohibit federal prosecutors from disclosing information from grand jury testimony and criminal investigative wiretaps to intelligence and national defense officials even if that information indicated that terrorists were planning a future attack, unless such officials were actually assisting with the criminal investigation. Sections 203(a) and (b) of the USA PATRIOT Act, however, eliminated these